(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

552374

(43) 国際公開日
2004 年10 月21 日 (21.10.2004)

PCT

(10) 国際公開番号
WO 2004/090738 A1

(51) 国際特許分類[7]: G06F 15/00, H04L 9/32

(21) 国際出願番号: PCT/JP2004/005205

(22) 国際出願日: 2004 年4 月12 日 (12.04.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-106420 2003 年4 月10 日 (10.04.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真1006番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 里村 尚 (SATOMURA, Takashi). 三田村 俊朗 (MITAMURA, Toshiro). 相澤 里香 (AIZAWA, Rika). 板原 美佐紀 (ITAHARA, Misaki).

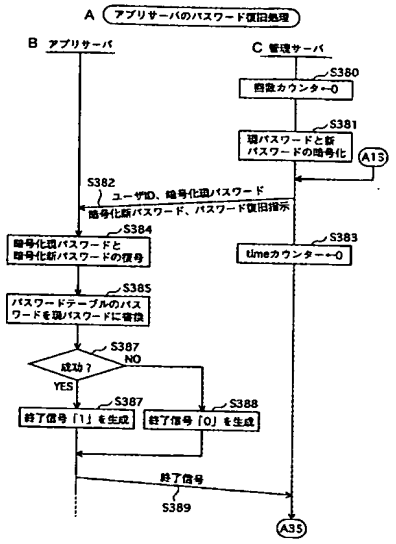
(74) 代理人: 中島 司朗 (NAKAJIMA, Shiro); 〒5310072 大阪府大阪市北区豊崎三丁目2番1号淀川5番館6F Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

[続葉有]

(54) Title: PASSWORD CHANGE SYSTEM

(54) 発明の名称: パスワード変更システム



A...PASSWORD RESTORATION BY APPLICATION SERVER
B...APPLICATION SERVER
C...MANAGEMENT SERVER
S380...COUNTER ← 0
S381...ENCRYPT CURRENT PASSWORD AND NEW PASSWORD
S382...SEND USER ID, ENCRYPTED CURRENT PASSWORD, ENCRYPTED NEW PASSWORD AND ISSUE INSTRUCTION TO RESTORE PASSWORD
S384...DECRYPT ENCRYPTED CURRENT PASSWORD AND ENCRYPTED NEW PASSWORD
S383...time COUNTER ← 0
S385...REWRITE PASSWORD IN PASSWORD TABLE TO CURRENT PASSWORD
S386...SUCCESSFUL?
S387...GENERATE TERMINATION SIGNAL "1"
S388...GENERATE TERMINATION SIGNAL "0"
S389...TERMINATION SIGNAL

(57) Abstract: A management server that can unify passwords for a plurality of application servers which authenticate a user by using the same password even if one of the application servers fails to change the password. If one of the application servers has failed to change the password, the management server restores the original password of an application server where the password has already been changed.

(57) 要約: 同一のパスワードにより、利用者の正当性を認証する複数のアプリサーバにおいて、複数のアプリサーバのうち何れかがパスワードの変更に失敗した場合でも、複数のアプリサーバのパスワードを統一することのできる管理サーバを提供することを目的とする。
管理サーバはパスワード変更を行う際、何れかのアプリサーバでパスワード変更が失敗した場合に、既にパスワードの変更を終えているアプリサーバのパスワードを元のパスワードに戻す。

WO 2004/090738 A1

SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

パスワード変更システム

技術分野

本発明は、パスワード変更システムに関する。

背景技術

従来、利用者に複数のサービスを提供する場合に、サービスを提供する各アプリケーションプログラムが、同一のパスワードを用いて、利用者の正当性を認証することが広く行われている。

このように、複数のサービスに対して同一パスワードを使用する場合において、安全性を確保するため、利用者はしばしばパスワードの変更を行う必要がある。

特許文献１では、同一のパスワードを用いる複数のサービスのパスワード変更方法が開示されている。このパスワード変更方法によると、パスワード管理装置は、サービスを提供する各アプリケーションプログラムを順次起動し、パスワードの変更を指示する。この際に、複数のプリケーションプログラムのうち、何れかが正常にパスワードを変更できないという障害が発生することがある。

パスワードが正常に変更できない場合としては、例えば、システムの外部ディスクのハード障害や瞬断などの電源不良、あるいはネットワークケーブルの接続不良などの場合が有り得る。

このような障害が発生すると、パスワード管理装置は、正常にパスワード変更できないアプリケーションプログラムについては、利用者が該当するサービスを利用するためにアプリケーションプログラムを再起動したときに、利用者に再度のパスワード変更の操作を促す。

そのため、前記アプリケーションプログラムの再起動を契機として、複数のサービスに対するパスワードの整合性を維持することが可能である。

しかしながら、特許文献１の方法では、パスワード変更に失敗したサ

ービスのパスワードは、次にアプリケーションを起動するまで他のサービスと同一のパスワードには保たれていないという問題が発生している。

特許文献１　特開２００２－169777号公報

発明の開示

そこで本発明はかかる問題点に鑑みてなされたものであり、複数のアプリケーション装置のうち何れかがパスワードの変更に失敗した場合でも、複数のアプリケーション装置のパスワードを統一することのできる管理サーバ装置、アプリケーション装置、パスワード変更システムを提供することを目的とする。

上記目的を達成するために本発明は、一のパスワードにより認証した一の利用者へ各サービスを提供する複数のアプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置であって、全てのアプリケーション装置のパスワードの更新を試みる第１手段と、各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第２手段と、不可能と判断されるアプリケーション装置が少なくとも１台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第３手段とを備える。

この構成によると、前記第２手段によりパスワードの更新が不可能であると判断されるアプリケーション装置が存在すると判断される場合でも、全てのアプリケーション装置のパスワードを更新前のものとすることで、複数のアプリケーション装置のパスワードの統一を保つことができる。

前記管理サーバ装置は、さらに、利用者装置からパスワードの更新の要求を受信する第４手段を含み、前記第１手段は、受信した前記更新の要求に基づいて、パスワードの更新を試みるとしてもよい。

この構成により、前記管理サーバ装置は、利用者の意思に基づきパスワードの更新を試みることができる。

また、前記管理サーバ装置において、前記第１手段は、全てのアプリケーション装置に対してパスワードの更新を指示し、前記第２手段は、

各アプリケーション装置について、パスワードの更新が失敗したか否かを判断し、前記第３手段は、少なくとも１台のアプリケーション装置について、更新が失敗したと判断される場合に、パスワードの更新が成功した他のアプリケーション装置に対して、更新前のパスワードへの復元を指示する。

これによると、前記第２判断手段は、何れかのアプリケーション装置のパスワード更新が失敗したか否かを判断し、前記第３判断手段は、少なくとも１台のアプリケーション装置のパスワード更新が失敗したと判断される場合に、パスワード更新が成功したアプリケーション装置に対し、更新前のパスワードへの復元を指示するので、前記アプリケーション装置のうち何れかが、パスワードの更新に失敗した場合にも、全てのアプリケーション装置のパスワードを速やかに統一することができる。

本発明において、前記第４手段は、利用者の新パスワードと旧パスワードとを含む前記更新の要求を受信し、前記第１手段は、受信した更新の要求に含まれる新パスワードと旧パスワードとを含む更新の指示を生成し、生成した前記更新の指示を全てのアプリケーション装置に対して送信することを特徴とする。

この構成によると、前記第４手段は利用者から前記新パスワードを含む前記パスワード更新の指示を受け付ける。これにより、利用者自身が任意の新パスワードを指定することができる。

また、本発明において、前記第２手段は、各アプリケーション装置からのパスワードの更新の成功又は失敗を示す応答を受信する応答受信部と、受信した前記応答が成功を示す場合に、当該アプリケーション装置についてパスワードの更新が成功したと断定し、受信した前記応答が失敗を示す場合に、当該アプリケーション装置についてパスワードの更新が失敗したと断定する断定部とを含むことを特徴とする。

この構成によると、前記応答受信部は、各アプリケーション装置からの応答を受信し、前記判断部は、前記応答が失敗を示す場合にアプリケーション装置のパスワード変更が失敗であると断定する。これにより、

各アプリケーション装置のパスワード更新の失敗を正確に検出することができる。

また、本発明は、前記第２手段が、時間の経過に伴って経過時間を計測する計時部と、前記第１手段による更新の指示の送信の時点において、計時部により計測される経過時間を初期値にリセットする初期化部と、各アプリケーション装置からのパスワードの更新の成功又は失敗を示す応答を待ち受ける待受部と、計測された経過時間が、所定のしきい値より大きいか否かを判断する判断部と、判断部により経過時間が前記しきい値と等しいか又は小さいと判断され、かつ待受部により各アプリケーション装置からの応答を受信し、かつその応答が成功を示す場合に、当該アプリケーション装置について、パスワードの更新が成功したと断定し、その他の場合に、当該アプリケーション装置について、パスワードの更新が失敗したと断定する断定部とを含むことを特徴とする管理サーバ装置である。

この構成によると、前記断定部は、前記閾値を超えても、前記応答を受信しない場合をパスワード変更の失敗と断定する、このため、前記閾値以上の無駄な待ち時間を削減できる。

本発明は、前記第１手段は、全てのアプリケーション装置に対してパスワードの更新の準備を指示し、前記第２手段は、各アプリケーション装置について、パスワードの更新の準備が未完了か否かを判断し、前記第３手段は、少なくとも１台のアプリケーション装置について、更新の準備が未完了と判断される場合に、更新の準備が完了した他のアプリケーション装置に対して、前記更新の準備の指示を取り消すことを特徴とする管理サーバ装置でもある。

この構成によると、パスワード更新の準備が未完了のアプリケーション装置が１つでも存在すると、前記パスワード更新の準備が完了したアプリケーション装置のパスワード更新の準備を取り消す。これにより、全てのアプリケーション装置のパスワード更新の準備が完了するまで、各アプリケーション装置のパスワード更新は実行されないため、ハード

ディスクへの無駄な書き込みを回避できる。

本発明において、前記第４手段は、利用者の新パスワードと旧パスワードとを含む前記更新の要求を受信し、前記第１手段は、受信した更新の要求に含まれる新パスワードと旧パスワードとを含む更新の準備の指示を生成し、生成した前記更新の準備の指示を全てのアプリケーション装置に対して送信することを特徴とする。

この構成によると、前記第４手段は利用者から前記新パスワードを含む前記パスワード更新の指示を受け付ける。これにより、利用者自身が任意の新パスワードを指定することができる。

また、本発明の管理サーバ装置において、前記第２手段は、アプリケーション装置からのパスワードの更新の準備の完了又は未完了を示す応答を受信する応答受信部と、受信した前記応答が完了を示す場合に、当該アプリケーション装置についてパスワードの更新の準備が完了したと断定し、受信した前記応答が未完了を示す場合に、当該アプリケーション装置についてパスワードの更新の準備が未完了であると断定する断定部とを含むことを特徴とする。

この構成によると、前記応答受信部は、各アプリケーション装置からの応答を受信し、前記判断部は、前記応答が未完了を示す場合にアプリケーション装置のパスワード変更準備が未完了であると断定する。これにより、各アプリケーション装置のパスワード更新準備の未完了を正確に検出することができる。

本発明において、前記第２手段は、時間の経過に伴って経過時間を計測する計時部と、前記第１手段による更新の準備の指示の送信の時点において、計時部により計測される経過時間を初期値にリセットする初期化部と、アプリケーション装置からのパスワードの更新の準備の完了又は未完了を示す応答を待ち受ける待受部と、計測された経過時間が、所定のしきい値より大きいか否かを判断する判断部と、判断部により経過時間が前記しきい値と等しいか又は小さいと判断され、かつ待受部によりアプリケーション装置からの応答を受信し、かつその応答が完了を示

す場合に、パスワードの更新の準備が完了したと断定し、その他の場合に、パスワードの更新の準備が未完了であると断定する断定部とを含むことを特徴とする。

この構成によると、前記閾値を超えても、前記応答を受信しない場合をパスワード変更の失敗と断定することにより、前記閾値以上の無駄な待ち時間を削減できる。

本発明である前記管理サーバ装置は、さらに、前記第２手段によりパスワードの更新が不可能と判断される場合に、元のパスワードに戻す旨のメッセージを前記利用者装置へ送信するメッセージ送信手段を含むことを特徴とする。

この構成によると、前記メッセージ送信手段は、前記利用者装置へ前記メッセージを送信するため、利用者は、使用すべきパスワードが更新前のものであることを知ることができる。

前記管理サーバ装置は、さらに、各アプリケーション装置について、メインテナンス中であるか否かを記憶している管理記憶手段を備え、前記第１手段は、メインテナンス中のアプリケーション装置が存在しない場合に、パスワードの更新を試みることを特徴とする。

この構成によると、前記第１手段は、メインテナンス中のアプリケーション装置が存在しない場合にパスワード更新を試みるため、メインテナンス中のアプリケーション装置のパスワード更新により、その他のアプリケーション装置のパスワード変更が妨げられることを予め回避することができる。

また、前記第１手段は、メインテナンス中のアプリケーション装置が存在する場合に、パスワードの更新を中止し、前記管理サーバ装置は、さらに、前記第１手段によりパスワードの更新が中止される場合に、パスワードの更新を中止する旨のメッセージを前記利用者装置へ送信するメッセージ送信手段を含むことを特徴とする。

この構成によると、前記メッセージ送信手段は、前記利用者装置へパスワードの更新を中断する旨のメッセージを送信するので、利用者は、

パスワード更新ができないことを確実に知ることができる。

また、本発明において、前記アプリケーション装置は、第１ネットワークを介して、前記管理サーバ装置と接続されており、前記利用者装置は、第１ネットワークに接続されていない第２ネットワークを介して、前記管理サーバ装置と接続されていることを特徴とする。

この構成によると、前記アプリケーション装置と前記利用者装置は、前記管理サーバ装置を介して接続されているため、前記管理サーバ装置は、前記アプリケーション装置と前記利用者装置の間の通信を監視することができる。

本発明において、前記第１ネットワーク及び前記第２ネットワークは、イントラネットであることを特徴とする。

この構成によると、前記アプリケーション装置と前記利用者装置とはそれぞれ異なるイントラネットを介して、管理サーバ装置と接続されているため、インターネットで普及している技術を利用して、容易に構成できる。

また、本発明において、前記管理サーバ装置と、各アプリケーション装置とは、専用線を介して、接続されており、パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、各アプリケーション装置との間で、パスワードの更新のための情報を送受信し、各サービスの提供の際には、前記管理サーバ装置は、第１及び第２ネットワークを介して、前記利用者装置と各アプリケーション装置との間で、前記サービスに係る情報の送受信を中継するとしてもよい。

この構成によると、前記管理サーバ装置は、パスワードの更新の際には、前記専用線を介して、各アプリケーション装置との間で、パスワードの更新のための情報を送受信する。専用線によりる通信は、第三者による盗聴の危険性が少ないので、パスワード更新の際の情報の送受信の暗号化の処理を省略することができる。

また、各サービスの提供の際には、前記管理サーバ装置は、第１及び第２ネットワークを介して、前記利用者装置と各アプリケーション装置

との間で、前記サービスに係る情報の送受信を中継するため、パスワード更新のための情報の送受信と前記サービスに係る情報の送受信は互いに影響を及ぼすことがない。

また、本発明における前記アプリケーション装置及び前記利用者装置は、ネットワークを介して、前記管理サーバ装置と接続されており、前記管理サーバ装置は、さらに、アプリケーションの種類と、各アプリケーション装置のネットワーク上における位置情報とを対応付ける対応テーブルを記憶している記憶手段と、前記利用者装置から、アプリケーションを示す種類情報と処理の内容を示す処理情報とを受信する受信手段と、前記対応テーブルを用いて、受信した種類情報に対応するアプリケーション装置の位置情報を取得する取得手段と、取得した位置情報により示されるアプリケーション装置に対して、前記処理情報を送信する送信手段とを含むとしてもよい。

この構成によると、前記取得手段は前記対応テーブルを用いて前記種類情報に対応するアプリケーション装置の位置情報を取得し、前記送信手段は、前記位置情報により示されるアプリケーション装置に対して、前記利用者装置から受信した前記処理情報を送信する。これにより、前記管理サーバ装置は、前記利用者装置から送信された処理情報をアプリケーション装置へ正確に転送できる。

また、前記ネットワークは、インターネットであるとしてもよい。

この構成によると、前記管理サーバ装置は、インターネットを介して遠隔地に存在する利用者装置と各アプリケーション装置との間で前記処理情報を転送することができる。

本発明は、更新後の新パスワードが、利用者に最初に割り当てられた初期パスワードであり、前記第１手段は、全てのアプリケーション装置の初期パスワードへの更新を試み、前記第２手段は、各アプリケーション装置について、初期パスワードへの更新が不可能か否かを判断し、前記第３手段は、不可能と判断されるアプリケーション装置が少なくとも１台存在する場合に、全てのアプリケーション装置のパスワードを更新

前のものとすることを特徴とする管理サーバ装置でもある。

この構成によると、前記第１手段は、前記初期パスワードへの更新を試みる。これにより、利用者による新パスワードの指定ができない場合でも、パスワードの更新を試みることができる。

本発明は、一のパスワードにより認証した一の利用者へサービスを提供し、管理サーバ装置からの指示によりパスワードを更新するアプリケーション装置であって、更新前のパスワードを記憶している旧パスワード記憶手段と、利用者の認証に用いるパスワードを記憶している認証用パスワード記憶手段と、管理サーバ装置から、パスワードを更新前のものに復元する復元指示を受信する受信手段と、前記復元指示を受信すると、旧パスワード記憶手段から更新前のパスワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きする書込手段とを備えることを特徴とするアプリケーション装置である。

この構成によると、管理サーバ装置から復元指示を受信すると、旧パスワード記憶手段の記憶している旧パスワード記憶手段から更新前のパスワードを読み出し、読み出したパスワードを認証用パスワードパスワード記憶手段に上書きするため、管理サーバ装置の指示により、認証用のパスワードを更新前のパスワードに速やかに変更することができる。

また、前記アプリケーション装置は、前記管理サーバ装置を介して、利用者の利用者装置との間で、前記サービスに関する情報の送受信を行うことを特徴とする。

この構成によると、前記アプリケーション装置は、前記管理サーバ装置を介して利用者端末との間で、情報の送受信を行うため、前記管理サーバ装置以外からの情報の受信を拒否することで、正当な利用者以外からのアクセスを回避できる。

本発明のアプリケーション装置は、メインテナンス中である場合に、当該旨を前記管理サーバ装置に対して通知することを特徴とする。

この構成によると、前記アプリケーション装置は、メインテナンス中である旨をあらかじめ管理サーバ装置へ通知しているので、前記管理サ

ーバ装置は、前記アプリケーション装置がメインテナンス中であることを事前に認識しており、当該アプリケーション装置に対する情報の送信及び指示の送信を中止又は延期することができる。

前記アプリケーション装置は、第１ネットワークを介して、前記管理サーバ装置と接続されており、前記利用者装置は、第１ネットワークに接続されていない第２ネットワークを介して、前記管理サーバ装置と接続されていることを特徴とする。

この構成によると、前記アプリケーション装置と前記利用者装置は、前記管理サーバ装置を介して接続されているため、前記管理サーバ装置は、前記アプリケーション装置と前記利用者装置の間の通信を監視することができる。

また、前記アプリケーション装置及び前記管理サーバ装置は、専用線を介して接続されており、パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、前記管理サーバとの間で、パスワードの更新のための情報を送受信し、各サービスの提供の際には、第１及び第２ネットワークを介して、前記サービスに係る情報を送受信することを特徴とするとしてもよい。

この構成によると、前記アプリケーション装置は、パスワード更新に関する情報の送受信には前記専用線を使用するため、第三者による盗聴が行われにくく、通信の安全性が高い。

また、各サービスに係る情報の送受信には第１ネットワーク及び第２ネットワークを使用するため、パスワード更新に関する情報の送受信とサービスに係る情報の送受信とは互いに影響を及ぼさない。

また、本発明における前記アプリケーション装置及び前記利用者装置は、インターネットを介して、前記管理サーバ装置と接続されていることを特徴とする。

この構成によると、前記アプリケーション装置及び前記利用者装置はインターネットを介して前記管理サーバ装置に接続されているため、前記アプリケーション装置、前記利用者装置及び前記管理サーバ装置がそ

れぞれ遠隔地に存在している場合でも、情報の送受信を行うことができる。

本発明は、利用者の端末装置と、一のパスワードにより認証した一の利用者の端末装置へ各サービスを提供する複数のアプリケーション装置と、前記アプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置とから構成されるパスワード更新システムであって、前記管理サーバ装置は、全てのアプリケーション装置のパスワードの更新を試みる第１手段と、各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第２手段と、不可能と判断されるアプリケーション装置が少なくとも１台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第３手段とを備え、各アプリケーション装置は、更新前のパスワードを記憶している旧パスワード記憶手段と、利用者の認証に用いるパスワードを記憶している認証用パスワード記憶手段と、管理サーバ装置から、パスワードを更新前のものに復元する復元指示を受信する受信手段と、前記復元指示を受信すると、旧パスワード記憶手段から更新前のパスワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きする書込手段とを備えることを特徴とする。

この構成により、複数のアプリケーション装置のうち何れかがパスワード更新不可能と判断される場合においても、全てのアプリケーション装置のパスワードを更新前のものとすることにより、全てのアプリケーション装置のパスワードの統一を保つことができる。

本発明における前記端末装置と各アプリケーション装置とは、前記管理サーバ装置を介して、情報の送受信を行うことを特徴とする。

この構成によると、前記アプリケーション装置は、前記管理サーバ装置を介して利用者端末との間で、情報の送受信を行うため、前記管理サーバ装置以外からの情報の受信を拒否することで、正当な利用者以外からのアクセスを回避できる。

また、前記アプリケーション装置は、第１ネットワークを介して、前

記管理サーバ装置と接続されており、前記利用者装置は、第１ネットワークに接続されていない第２ネットワークを介して、前記管理サーバ装置と接続されていることを特徴とする。

この構成によると、前記アプリケーション装置と前記利用者装置は、前記管理サーバ装置を介して接続されているため、前記管理サーバ装置は、前記アプリケーション装置と前記利用者装置の間の通信を監視することができる。

また、前記パスワード更新システムにおいて、前記第１ネットワーク及び前記第２ネットワークは、イントラネットであることを特徴とする。

この構成によると、前記アプリケーション装置と前記利用者装置とはそれぞれ異なるイントラネットを介して、管理サーバ装置と接続されているため、インターネットで普及している技術を利用して、容易に構成できる。

前記パスワード更新システムにおいて、前記管理サーバ装置と、各アプリケーション装置とは、専用回線を介して、接続されており、パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、前記管理サーバとの間で、パスワードの更新のための情報を送受信し、各サービスの提供の際には、第１及び第２ネットワークを介して、前記サービスに係る情報を送受信するとしてもよい。

この構成によると、前記アプリケーション装置は、パスワード更新に関する情報の送受信には前記専用線を使用するため、第三者による盗聴が行われにくく、通信の安全性が高い。

また、各サービスに係る情報の送受信には第１ネットワーク及び第２ネットワークを使用するため、パスワード更新に関する情報の送受信とサービスに係る情報の送受信とは互いに影響を及ぼさない。

本発明のパスワード更新システムは、前記アプリケーション装置及び前記利用者装置は、ネットワークを介して、前記管理サーバ装置と接続されており、前記管理サーバ装置は、さらに、アプリケーションの種類と、各アプリケーション装置のネットワーク上における位置情報とを対

応付ける対応テーブルを記憶している記憶手段と、前記利用者装置から、アプリケーションを示す種類情報と処理の内容を示す処理情報とを受信する受信手段と、前記対応テーブルを用いて、受信した種類情報に対応するアプリケーション装置の位置情報を取得する取得手段と、取得した位置情報により示されるアプリケーション装置に対して、前記処理情報を送信する送信手段とを含むことを特徴とするとしてもよい。

この構成によると、前記取得手段は前記対応テーブルを用いて前記種類情報に対応するアプリケーション装置の位置情報を取得し、前記送信手段は、前記位置情報により示されるアプリケーション装置に対して、前記利用者装置から受信した前記処理情報を送信する。これにより、前記管理サーバ装置は、前記利用者装置から送信された処理情報をアプリケーション装置へ正確に転送できる。

また、前記ネットワークは、インターネットであることを特徴とする。

この構成によると、前記アプリケーション装置及び前記利用者装置はインターネットを介して前記管理サーバ装置に接続されているため、前記アプリケーション装置、前記利用者装置及び前記管理サーバ装置がそれぞれ遠隔地に存在している場合でも、情報の送受信を行うことができる。

図面の簡単な説明

図１は、パスワード変更システムの構成図である。

図２は、ユーザ端末１００の構成を示すブロック図である。

図３は、記憶部１１０に記憶されている情報の一例を示す。

図４は、本実施の形態で、各機器間で送受信される情報の形態を示す。

図５は、ユーザ端末１００に接続されているモニタに表示されるログイン画面とメニュー画面の一例を示す。

図６は、ユーザ端末１００に接続されているモニタに表示される精算画面と精算終了画面の一例を示す。

図７は、ユーザ端末１００に接続されているモニタに表示されるパスワード変更画面と変更完了画面の一例を示す。

図８は、ユーザ端末１００に接続されているモニタに表示される変更失敗画面と強制終了画面の一例を示す。

図９は、アプリサーバ２００の構成を示すブロック図である。

図１０は、情報記憶部２１０に記憶されている情報の一例である。

図１１は、パスワードテーブル２２１の詳細を示している。

図１２は、アプリログインテーブル２３１の詳細を示している。

図１３は、管理サーバ６００の構成を示すブロック図である。

図１４は、情報記憶部６１０に記憶されている情報の一例を示す。

図１５は、ログインテーブル６３１の詳細を示す。

図１６は、ルーティングテーブル６４１の詳細を示す。

図１７は、パスワード変更テーブル６５１の詳細を示す。

図１８は、管理サーバ６００の表示部６１３に表示されるエラー画面の一例である。

図１９は、ユーザ端末１００、管理サーバ６００及びアプリサーバ２００による動作を示したフローチャートである。

図２０は、ユーザ端末１００、管理サーバ６００及びアプリサーバ２００による動作を示したフローチャートである。図１９より続く。

図２１は、ユーザ端末１００、管理サーバ６００及びアプリサーバ２００による動作を示したフローチャートである。図１９より続く。

図２２は、ユーザ端末１００、管理サーバ６００及びアプリサーバ２００による動作を示したフローチャートである。図１９より続く。

図２３は、ユーザ端末１００、管理サーバ６００及びアプリサーバ２００による動作を示したフローチャートである。図１９より続く。

図２４は、ユーザ端末１００、管理サーバ６００及びアプリサーバ２００による動作を示したフローチャートである。図１９より続く。

図２５は、ユーザ端末１００、管理サーバ６００及びアプリサーバ２００による動作を示したフローチャートである。図１９より続く。

図２６は、ユーザ端末１００、管理サーバ６００及びアプリサーバ２００による動作を示したフローチャートである。図１９より続く。

図２７は、管理サーバ６００によるパスワード変更処理の動作を示すフローチャートである。

図２８は、管理サーバ６００によるパスワード変更処理の動作を示すフローチャートである。図２７より続く。

図２９は、管理サーバ６００によるパスワード変更処理の動作を示すフローチャートである。図２７より続く。

図３０は、アプリサーバ２００のパスワード変更処理の動作を示すフローチャートである。

図３１は、アプリサーバ２００のパスワード変更処理の動作を示すフローチャートである。図３０より続く。

図３２は、管理サーバ６００によるパスワード復旧の動作を示すフローチャートである。

図３３は、アプリサーバ２００のパスワード復旧の動作を示すフローチャートである。

図３４は、アプリサーバ２００のパスワード復旧の動作を示すフローチャートである。図３３より続く。

図３５は、二つの機器間の相互認証の動作を示したフローチャートである。

図３６は、二つの機器間の相互認証の動作を示したフローチャートである。図３５より続く。

図３７は、実施の形態１における、パスワード変更の実行中の各アプリサーバ２００の記憶しているパスワードを示している。

図３８は、実施の形態２の構成を示した構成図である。

図３９は、実施の形態２における管理サーバ６００ｂの構成を示すブロック図である。

図４０は、実施の形態３の構成を示した構成図である。

図４１は、実施の形態２における管理サーバ６００ｃの構成を示すブロック図である。

図４２は、変形例（１）におけるパスワードテーブル６２１ｂの詳細を

示す。

図４３は、変形例（６）におけるルーティングテーブル６４１ｂの詳細を示す。

発明を実施するための最良の形態

１．実施の形態１

以下、本発明の実施の形態１について図面を用いて詳細に説明する。

１．１パスワード変更システムの概要

本発明におけるパスワード変更システムは、図１に示すように、ユーザ端末１００、第１アプリサーバ２００ａ、第２アプリサーバ２００ｂ、第３アプリサーバ２００ｃ、第４アプリサーバ２００ｄ及び管理サーバ６００から構成される。各装置は、インターネット２０に接続されている。

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、それぞれ、出張費精算、休暇申請、会議室予約、従業員購入のサービスを提供する。

管理サーバ６００及び第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、あらかじめ正当な利用者のユーザＩＤとを記憶している。

利用者は、ユーザ端末１００を用いて、インターネット２０と管理サーバ６００とを介して、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄの提供するサービスを利用する。

このとき、ユーザ端末１００は、管理サーバ６００に利用者のユーザＩＤとパスワードを送信する。

管理サーバ６００及び第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、ユーザＩＤとパスワードを検証し、ユーザ端末１００の利用者が正当な利用者であることを認証し、各アプリサーバは、それぞれが備えるサービスを提供する。

また、管理サーバ６００は、ユーザ端末１００からパスワード変更の指示を受信し、ユーザ端末１００から、現在のパスワードと新しいパスワードとを受信する。管理サーバ６００は、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄへ、受け取った新しいパスワードを順次送

信し、パスワードの変更を指示する。

ここで、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄの何れかで、パスワードの変更が正常に行われなかった場合、管理サーバ６００は、既にパスワード変更が終了しているアプリサーバに現在のパスワードを送信し、現在のパスワードへパスワードを変更し直すように指示する。

以下の説明において第１アプリサーバ２００ａ～第４アプリサーバ２００ｄを特に区別しない場合及び第１アプリサーバ２００ａ～第４アプリサーバ２００ｄ全てに共通する場合、これらを単にアプリサーバ２００と呼称する。

１．２　ユーザ端末１００

ユーザ端末１００は、図２に示すように、送受信部１０１、認証部１０３、制御部１０７、記憶部１１０、入力部１１２及び画像表示部１１３から構成される。

ユーザ端末１００は、具体的には図示されていないマイクロプロセッサ、ＲＡＭ、ＲＯＭ及びハードディスクから構成されている。前記ＲＡＭ、ＲＯＭ及びハードディスクにはコンピュータプログラムが記憶されており、前記マイクロプロセッサがこれらのコンピュータプログラムに従って動作することにより、ユーザ端末１００はその機能を果たす。

（１）記憶部１１０

記憶部１１０は、ハードディスク、ＲＡＭ及びＲＯＭから構成され、各種情報を記憶している。

一例として、図３に示すように、アプリ番号表１２０、端末ＩＤ１３０、秘密鍵１３５、公開鍵証明書１３６、ＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）１３７及び認証局公開鍵１３８を記憶している。

アプリ番号表１２０は、アプリサーバ２００及び管理サーバ６００の提供するサービスと各サービスに割り当てられたアプリ番号とを対応付ける表である。アプリ番号「００１」は、出張費精算サービスを示す識

別番号であり、アプリ番号「００２」は休暇申請サービスを示す識別番号である。アプリ番号「００３」は、会議室予約サービスを示す識別番号であり、アプリ番号「００４」は、従業員購入サービスを示す識別番号である。アプリ番号「００５」は、ログイン処理、パスワードの変更など管理サーバの提供するサービスを示す識別番号である。

端末ＩＤ１３０は、ユーザ端末１００に固有の識別情報である。

公開鍵証明書１３６は、秘密鍵１３５と対になる公開鍵の正当性を証明するものであり、証明書ＩＤ、前記公開鍵及び認証局による署名データを含む。認証局の署名データは、認証局の秘密鍵を用いて、前記公開鍵に署名生成アルゴリズムＳを施して、生成したものである。ここで、認証局は、第三者機関であり、パスワード変更システムに属する各機器の公開鍵証明書を発行する。なお、署名生成アルゴリズムＳは一例として、有限体上のＥｌＧａｍａｌ署名である。ＥｌＧａｍａｌ署名については、公知であるので説明を省略する。

ＣＲＬ１３７は、認証局により発行され、無効になった公開鍵証明書の証明書ＩＤを含む。

認証局公開鍵１３８は、認証局の秘密鍵と対になる公開鍵である。

（２）送受信部１０１

送受信部１０１は、インターネット２０に接続されている外部機器と制御部１０７及び認証部１０３の間で情報の送受信を行う。

送受信部１０１は、ユーザ端末１００及び管理サーバ６００のＩＰアドレスを記憶している。

送受信部１０１が送受信する各種の情報は、図４に示すパケット１４０のような形体である。パケット１４０は、送信先アドレス１４１、送信元アドレス１４２及びデータ部１４３から構成される。送信先アドレスは、送信先のＩＰアドレス、送信元アドレス１４２は、送信元のＩＰアドレスである。データ部１４３は、一例として、アプリ番号１４６、端末ＩＤ１４７及びデータ１４８を含む。

アプリ番号１４６は、第１アプリサーバ２００ａ～第４アプリサーバ

及び管理サーバ６００の提供するサービスの種類と対応しており、これは、アプリ番号表１２０に含まれるアプリ番号と同一である。

送受信部１０１は、制御部１０７から、アプリ番号１４６、端末ＩＤ１４７及びデータ１４８からなるデータ部１４３を受け取り送信の指示を受けると、受け取ったデータ部１４３に送信元アドレスとしてユーザ端末１００のＩＰアドレスを設定し、送信先アドレスとして管理サーバ６００のＩＰアドレスを設定して送信する。

ここでは、説明を容易にするために、データ部１４３に含まれるアプリ番号１４６、端末ＩＤ１４７及びデータ１４８を列挙しているが、実際には、データ部１４３は、可変長であるが最大ビット長が決まっているため、データ部１４３が最大ビット長を超える場合は、データ部１４３を分割し、分割されたデータ部１４３それぞれに、送信先アドレスと送信元アドレスとを設定し、送信する。

（３）入力部１１２

入力部１１２は、キーボード、マウスといった周辺機器と接続されており、利用者による周辺機器の操作を受け付け、受け付けた操作に応じた操作指示情報を制御部１０７へ出力する。

（４）制御部１０７

制御部１０７は、上記のプロセッサがコンピュータプログラムに従って動作することにより、ユーザ端末１００で実行する各種の情報処理を制御する。

本願に関しては、制御部１０７は、入力部１１２から各種の操作指示情報を受け取る。受け取った操作指示情報により、ログイン処理、各種サービスの利用及びパスワードの変更処理等を行う。

また、これらの処理の途中で、管理サーバ６００からログイン画面データ、端末用メニュー画面データ、端末用精算画面データ、端末用精算完了画面データ、端末用パスワード変更画面データ、端末用変更完了画面データ、端末用変更失敗画面データ、端末用強制終了画面データ等の画面データ、各種サービス、パスワード変更、相互認証、暗号処理に関

する各種情報を受信し、受信した各種画面データ及び各種の情報を処理する。

上記の処理中に、制御部１０７が送受信部１０１を介して管理サーバ６００へ送信する情報は、図４に示すパケット１４０の形体をしている。制御部１０７は、記憶部１１０から端末ＩＤ１３０を読み出し、アプリ番号表１２０からアプリ番号を抽出し、読み出した端末ＩＤ１３０と抽出したアプリ番号と各種情報からなるデータ部１４３を生成する。生成したデータ部１４３を送受信部１０１へ出力し、送信を指示する。

以下の説明において、データ部１４３の生成についての説明は簡略化し、単にアプリ番号と端末ＩＤと各種情報と表現する。

以下に、ログイン処理、各種サービスの利用の処理及びパスワードの変更処理について、説明する。

（ログイン処理）

制御部１０７は、入力部１１２から、電子申請を示す操作指示情報を受け取ると、認証部１０３へ、管理サーバ６００との間の相互認証を指示する。

認証部１０３による相互認証が成立し、認証部１０３から、端末共通鍵を受け取り、受け取った端末共通鍵を記憶する。次に、送受信部１０１を介して、管理サーバ６００から、ログイン画面データを受信し、受信したログイン画面データからをログイン画面１５１を生成し、生成したログイン画面１５１を画像表示部１１３へ出力し、ログイン画面１５１の表示を指示する。図５に示すログイン画面１５１は、ここで表示される画面の一例である。ログイン画面データは、ログイン画面１５１を生成するためのデータでありＨＴＭＬにより記述される。

次に、入力部１１２を介して利用者の入力及びを受け付ける。送信ボタン１５４の押下を示す操作指示情報を受け取ると、パスワードボックス１５３に記入されたパスワードと端末共通鍵とを暗号処理部１０８へ出力し、暗号化を指示する。次に、暗号処理部１０８から暗号化パスワードを受け取り、記憶部１１０からアプリ番号「００５」と端末ＩＤ１

３０とを読み出す。読み出したアプリ番号「００５」と端末ＩＤ１３０と受け取った暗号化パスワードとユーザＩＤボックス１５２に入力されたユーザＩＤとを送受信部１０１へ出力し、管理サーバ６００への送信を指示する。

（各種サービスの利用）

次に、管理サーバ６００から、端末用メニュー画面データを受信し、受信した端末用メニュー画面データからメニュー画面１６１を生成し、生成したメニュー画面１６１を画像表示部１１３に出力し、メニュー画面１６１の表示を指示する。図５は、ここで表示される示すメニュー画面１６１の一例である。端末用メニュー画面データは、メニュー画面１６１を生成するためのデータであり、ＨＴＭＬにより記述される。

次に、入力部１１２から、メニュー画面１６１上に表示されるボタン１６２～１６６の押下を示す操作指示情報を受け取る。

制御部１０７は、入力部１１２からボタン１６２、１６３、１６４又は１６５の押下を示す操作指示情報を受け取り、それぞれ、出張費精算、休暇申請、会議室予約又は従業員購入のサービスの利用の処理を開始する。

ここでは、一例として、出張費精算サービスの利用についてのみ、具体的に説明する。

ボタン１６２の押下を示す操作指示情報を入力部１１２から受け取ると、制御部１０７は、記憶部１１０のアプリ番号表１２０から、アプリ番号「００１」を抽出し、端末ＩＤ１３０を読み出し、抽出したアプリ番号「００１」と読み出した端末ＩＤ１３０とを送受信部１０１を介して管理サーバ６００へ送信し、サービス開始を要求する。

次に、制御部１０７は、送受信部１０１を介して、管理サーバ６００から、ｗａｉｔメッセージ、端末用強制終了画面データ又は端末用精算画面データを受信する。端末用強制終了画面データ及び端末用精算画面データは、強制終了画面３２１及び精算画面１７１を生成するためのデータでありＨＴＭＬにより記述される。

ｗａｉｔメッセージを受信すると、画像表示部１１３を介して受信したｗａｉｔメッセージをモニタに表示し、次に、画像表示部１１３を介してメニュー画面１６１をモニタに表示し、メニューの選択の受付から処理をやり直す。

端末用強制終了画面データを受信すると、受信した端末用強制終了画面データから強制終了画面３２１を生成し、生成した強制終了画面３２１を画像表示部１１３へ出力し、強制終了画面３２１の表示を指示し、処理を終了する。図８に示す強制終了画面３２１は、ここで表示される画面の一例である。

端末用精算画面データを受け取ると、受け取った端末用精算画面データから精算画面１７１を生成し、生成した精算画面１７１画像表示部１１３へ出力し、精算画面１７１の表示を指示する。図６は、ここで表示される精算画面１７１の一例である。

次に、入力部１１２を介して利用者による入力を受け付ける。入力部１１２から、精算画面１７１上の送信ボタン１７３の押下を示す操作指示情報を受け取り、精算画面１７１上に入力されている入力データと端末共通鍵とを暗号処理部１０８へ出力し、暗号化を指示する。図４に示すデータ１４９はここで出力される入力データの一例であり、行き先、交通機関名、料金などを含む。

暗号処理部１０８から暗号化入力データを受け取り、記憶部１１０からアプリ番号「００１」と端末ＩＤ１３０とを読み出し、読み出したアプリ番号「００１」と端末ＩＤ１３０と受け取った暗号化入力データとを、送受信部１０１を介して管理サーバ６００へ送信する。

次に、管理サーバ６００から、端末用精算終了画面データを受信し、受信した端末用精算終了画面データから精算終了画面１８１を生成し、生成した精算終了画面１８１を画像表示部１１３へ出力し、表示を指示する。図６に示す精算終了画面１８１は、ここで表示される画面の一例である。端末用精算終了画面データは、精算終了画面を生成するためのデータであり、ＨＴＭＬにより記述される。

次に、入力部１１２から、精算終了画面１８１上のメニューボタン１８２又はログアウトボタン１８３の押下を示す操作指示情報を受け取る。

メニューボタン１８２の押下を示す操作指示情報を受け取ると、画像表示部１１３にメニュー画面１６１の表示を指示し、メニューの選択を受け付ける。

ログアウトボタン１８３の押下を示す操作指示情報を受け取ると、制御部１０７は、ログアウト通知を生成し、記憶部１１０からアプリ番号「００５」と端末ＩＤとを読み出し、読み出したアプリ番号「００５」と端末ＩＤとログアウト通知とを送受信部１０１を介して、管理サーバ６００へ送信し、処理を終了する。

（パスワード変更）

メニュー画面１６１上のボタン１６６の押下を示す操作指示情報を受け取ると、制御部１０７は、パスワードの変更を要求するパスワード変更指示を生成し、記憶部１１０からアプリ番号「００５」と端末ＩＤ１３０とを読み出し、読み出したアプリ番号「００５」と端末ＩＤ１３０と生成したパスワード変更指示とを、送受信部６０１を介して管理サーバ６００へ送信する。

次に、送受信部１０１を介して管理サーバ６００から、端末用パスワード変更画面データを受信する。受信した端末用パスワード変更画面データからパスワード変更画面１９１を生成し、生成したパスワード変更画面１９１を画像表示部１１３に出力し表示を指示する。図７は、ここで表示されるパスワード変更画面１９１の一例である。端末用パスワード変更画面データは、パスワード変更画面１９１を生成するためのデータであり、ＨＴＭＬにより記述される。

次に、入力部１１２を介して、利用者による入力を受け付ける。以下の説明において、利用者により空欄１９２に入力されるパスワードを現パスワード、空欄１９３及び１９４に入力されるパスワードを新パスワードと呼称する。

入力部１１２から送信ボタン１９５の押下を示す操作指示情報を受け

取ると、受け付けた現パスワード及び新パスワードと端末共通鍵とを暗号処理部１０８へ出力し、暗号化を指示する。次に、暗号処理部１０８から暗号化現パスワードと暗号化新パスワードとを受け取る。記憶部１１０から、アプリ番号「００５」と端末ＩＤ１３０とを読み出し、読み出したアプリ番号「００５」と端末ＩＤ１３０と受け取った暗号化現パスワードと暗号化新パスワードとを送受信部１０１を介して、管理サーバ６００へ送信する。

次に、管理サーバ６００から、端末用変更完了画面データ、端末用変更失敗画面データ又は端末強制終了画面データを受信する。端末用変更完了画面データ、端末用変更失敗画面データは、それぞれ変更完了画面３０１及び変更失敗画面３１１を生成するためのデータであり、一例として、ＨＴＭＬにより記述される。

端末用強制終了画面データを受信すると、受信した端末用強制終了画面データから強制終了画面３２１を生成し、生成した強制終了画面３２１を画像表示部１１３を介してモニタに表示し、処理を終了する。

端末用変更完了画面データを受信すると、受信した端末用変更完了画面データから変更完了画面３０１を生成し、生成した変更完了画面３０１を画像表示部１１３を介してモニタに表示する。図７は、ここで表示される変更完了画面３０１の一例を示している。

次に、入力部１１２を介して、利用者のボタン操作を受け付ける。入力部１１２から、変更完了画面３０１上のメニューボタン３０２の押下を示す操作指示情報を受け取ると、画像表示部１１３にメニュー画面１６１の表示を指示し、利用者によるメニューの選択へもどる。

ログアウトボタン３０３の押下を示す操作指示情報を受け取ると、制御部１０７は、ログアウト通知を生成し、記憶部１１０からアプリ番号「００５」と端末ＩＤ１３０とを読み出し、読み出したアプリ番号「００５」と端末ＩＤ１３０とログアウト通知とを送受信部１０１を介して、管理サーバ６００へ送信し、処理を終了する。

端末用変更失敗画面データを受信すると、制御部１０７は、受信した

端末用変更失敗画面データから変更失敗画面３１１を生成し、生成した変更失敗画面３１１を画像表示部１１３を介してモニタに表示する。図８は、ここで表示される変更失敗画面３１１の一例を示している。次に、入力部１１２を介して、利用者のボタン操作を受け付ける。入力部１１２から、変更失敗画面３１１上のメニューボタン３１２の押下を示す操作指示情報を受け取ると、画像表示部１１３にメニュー画面１６１の表示を指示し、メニューの選択の受け付けに戻る。

ログアウトボタン３１３の押下を示す操作指示情報を受け取ると、制御部１０７は、ログアウト通知を生成し、記憶部１１０からアプリ番号「００５」と端末ＩＤ１３０とを読み出し、読み出したアプリ番号「００５」と端末ＩＤ１３０とログアウト通知とを送受信部１０１を介して、管理サーバ６００へ送信し、処理を終了する。

（５）認証部１０３

認証部１０３は、制御部１０７と外部機器との通信に先だって、秘密鍵１３５と公開鍵証明書１３６とを用いて外部機器との間で相互認証を行い、相互認証が成功した場合のみ制御部１０７と外部機器との通信を許可し、外部装置と同一の端末共通鍵を生成する。ここで、外部機器とは、具体的には、管理サーバ６００である。

（６）暗号処理部１０８

暗号処理部１０８は、制御部１０７から各種情報と端末共通鍵とを受け取り暗号化を指示される。暗号化の指示を受け取ると、受け取った端末共通鍵を用いて受け取った各種情報に暗号化アルゴリズムＥ１を施して暗号化情報を生成し、生成した暗号化情報を制御部１０７へ出力する。

暗号処理部１０８が、制御部１０７から受け取る各種情報は、具体的には、パスワード、入力情報、現パスワード及び新パスワードである。

また、制御部１０７から各種の暗号化情報と端末共通鍵を受け取り、復号を指示される。復号の指示を受け取ると、暗号処理部は、受け取った暗号化情報に、端末共通鍵を用いて、復号アルゴリズムＤ２を施し、各種の情報を生成する。

ここで、復号アルゴリズムＤ２は、暗号化アルゴリズムＥ２により生成された暗号文を復号するアルゴリズムであり、暗号化アルゴリズムＥ１及びＥ２は一例としてＤＥＳ暗号方式などの共通鍵暗号方式を用いる。ＤＥＳ暗号方式については、公知であるので説明を省略する。

（７）画像表示部１１３

画像表示部１１３は、外部のモニタと接続されている。

画像表示部１１３は、制御部１０７から各種の画面を受け取り、画面の表示を指示される。受け取った画面から画像信号を生成し、垂直同期信号、水平同期信号を生成し、生成した垂直同期信号及び水平同期信号に合わせて、画像信号をモニターへ出力する。

１．３　アプリサーバ２００

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、ユーザ端末１００に対して、各種のサービスを提供する。本実施の形態では、第１アプリサーバ２００ａは、出張費精算、第２アプリサーバ２００ｂは休暇申請、第３アプリサーバ２００ｃは、会議室予約、第４アプリサーバ２００ｄは、従業員購入のサービスを提供する。

アプリサーバ２００は、図９の示すように、送受信部２０１、認証部２０３、制御部２０７、暗号処理部２０８、情報記憶部２１０、入力部２１２及び表示部２１３から構成される。

アプリサーバ２００は、具体的には図示されていないマイクロプロセッサ及びＲＡＭ、ＲＯＭなどから構成される。前記ＲＡＭ、ＲＯＭにはコンピュータプログラムが記憶されており、前記マイクロプロセッサがこれらのコンピュータプログラムの示す手順に従って動作することにより、アプリサーバ２００は、その機能を達成する。

（１）情報記憶部２１０

情報記憶部２１０は、ハードディスクユニットから構成され、一例として図１０に示すように、パスワードテーブル２２１、アプリログインテーブル２３１、秘密鍵２４２、公開鍵証明書２４３、ＣＲＬ２４４及び認証局公開鍵２４５を記憶している。また、具体的に図示していない

が、アプリサーバ２００が提供するサービスを実行するための各種プログラム及び画像データを記憶している。

パスワードテーブル２２１は、図１１に示すように、複数のパスワード情報２２３、２２４、２２５・・・から構成され、各パスワード情報は、ユーザＩＤ、氏名及びパスワードを含む。ユーザＩＤは、アプリサーバ２００の正当な利用者と１対１に対応しており、氏名は、ユーザＩＤと対応する利用者の氏名である。パスワードは、ユーザＩＤと対応する利用者がアプリサーバ２００の正当な利用者であるか否かを判断するための文字列又は数字列である。

アプリログインテーブル２３１は、図１２に示すように、複数のログイン情報２３２、２３３・・・から構成される。各ログイン情報は、ユーザＩＤ、氏名パスワード及び端末ＩＤを含む。

ユーザＩＤは、現在、アプリサーバ２００によるパスワード認証を終え、アプリサーバ２００の提供するサービスを利用中の利用者と対応しており、氏名及びパスワードは、ユーザＩＤと対応する利用者の氏名及びパスワードである。端末ＩＤは、利用者が現在使用しているユーザ端末に固有の識別情報である。

公開鍵証明書２４３は、秘密鍵２４２と対になる公開鍵の正当性を証明するものであり、証明書ＩＤ、前記公開鍵及び認証局による署名データを含む。

ＣＲＬ２４４及び認証局公開鍵２４５は、ユーザ端末１００の記憶しているＣＲＬ１３７及び認証局公開鍵１３８と同一のものであるので説明を省略する。

（２）送受信部２０１

送受信部２０１は、アプリサーバ２００のＩＰアドレス及び管理サーバ６００のＩＰアドレスを記憶している。

送受信部２０１は、制御部２０７及び認証部２０３と管理サーバ６００との間で情報の送受信を行う。

送受信部２０１が、制御部２０７と管理サーバ６００との間で送受信

する各種の情報は、図４に示すパケット１４０の形体をしている。制御部２０７から、アプリ番号、端末ＩＤ及び各種の情報からなるデータ部１４３を受け取り送信を指示される。

制御部２０７から送信を指示されると、受け取ったデータ部１４３に送信元としてアプリサーバ２００のＩＰアドレスを設定し、送信先としてアプリサーバ２００のＩＰアドレスを設定して送信する。

また、送受信部２０１は、管理サーバ６００以外の外部装置からの情報の受信を拒否する。具体的には、受信したパケットに含まれる送信元アドレスが管理サーバ６００のＩＰアドレスであるか否かを確認し、管理サーバ６００のＩＰアドレスでなければ受信したパケットを削除する。

（３）入力部２１２及び表示部２１３

入力部２１２は、操作者による情報及び指示の入力を受け付け、受け付けた情報及び受け付けた指示に応じた操作指示情報を制御部２０７へ出力する。

表示部２１３は、制御部２０７の制御により、各種情報を表示する。

（４）制御部２０７

制御部２０７は、上記のプロセッサがコンピュータプログラムに従って動作することにより、アプリサーバ２００００で実行する各種の情報処理を制御する。

制御部２０７は、管理サーバ６００から公開鍵証明書を受信し、受信した公開鍵証明書を認証部２０３へ出力し、管理サーバ６００との相互認証を指示する。認証部２０３による相互認証が成功し、認証部２０３からサーバ共通鍵を受け取ると、受け取ったサーバ共通鍵を記憶する。記憶したサーバ共通鍵用いて、秘密通信を行い、以下に説明する各処理において、安全に情報の送受信を行う。

また、制御部２０７は、アプリサーバ２００自身が提供するサービスを示すアプリ番号を記憶しており、以下の処理において、送受信部２０１を介して情報の送信を行う際、記憶しているアプリ番号と処理対象となっている利用者が使用しているユーザ端末１００の端末ＩＤと送信す

る情報とからなるデータ部１４３を生成し、生成したデータ部１４３を送受信部２０１へ出力する。以下の説明において、データ部１４３の生成については説明を省略し、単に、アプリ番号と端末ＩＤと各種情報と表現する。

制御部２０７は、管理サーバ６００から、アプリサーバ２００のアプリ番号と端末ＩＤとユーザＩＤと暗号化パスワードとサービス開始要求とを受信する。また、管理サーバ６００からアプリ番号と端末ＩＤとログアウト通知とを受信する。

制御部２０７は、管理サーバ６００からアプリサーバ２００と対応するアプリ番号と端末ＩＤとユーザＩＤと暗号化現パスワードと暗号化新パスワードとパスワード変更の指示を受信する。また、管理サーバ６００から、アプリサーバ２００と対応するアプリ番号とユーザＩＤと暗号化現パスワードと暗号化新パスワードとパスワード復旧の指示を受け取る。

以下に、制御部２０７の行うサービス提供の処理、パスワード変更の処理、パスワード復旧の処理及びログアウト処理について説明する。

（ｉ）サービス提供の処理

サービスの提供の処理において、制御部２０７は、管理サーバ６００から各種情報を受信するたびに、各種情報と供に受信するユーザ端末１００の端末ＩＤを含むログイン情報２３２が、アプリログインテーブル２３１内に存在することを確認し、ユーザ端末１００の利用者がログイン済みであることを確認する。以下のサービス提供の説明において、受信時のログイン済みの確認ついては、説明を省略する。

制御部２０７は、管理サーバ６００からアプリ番号と処理対象となっている利用者の使用しているユーザ端末１００の端末ＩＤとユーザＩＤと暗号化パスワードとサービス開始要求とを受信すると、サービス提供の処理を開始する。ここでは、一例として、第１アプリサーバ２００ａの提供する出張費精算のサービスについて説明する。

制御部２０７は、受信した暗号化パスワードと、相互認証により生成

されたサーバ共通鍵とを暗号処理部１０８へ出力し、復号を指示する。暗号処理部２０８からパスワードを受け取ると、パスワードテーブル２２１に受信したユーザＩＤとパスワードとを含むパスワード情報が存在するか否かを判断する。受け取ったユーザＩＤとパスワードとを含むパスワード情報がパスワードテーブル２２１内に存在しないと判断すると、制御部２０７は、管理サーバ６００の記憶しているパスワードと第１アプリサーバ２００ａが記憶しているパスワードが一致していないことを示すパスワードエラー信号と受信したユーザＩＤとを、管理サーバ６００へ送信し、サービス提供の処理を終了する。

受信したユーザＩＤとパスワードを含むパスワード情報２２３が存在すると判断すると、受信したユーザＩＤと暗号処理部２０８から受け取ったパスワードを含むパスワード情報２２３を選択する。次に、受信した端末ＩＤと抽出した端末ＩＤと選択したパスワード情報２２３とからログイン情報２３２を生成し、生成したログイン情報２３２をアプリログインテーブル２３１に追加して書き込む。

次に、制御部２０７は、情報記憶部２１０から精算画面データを読み出し、ログイン情報２３２からユーザＩＤと氏名を抽出し、読み出した精算画像データと抽出したユーザＩＤと氏名とを基に、端末用精算画面データを生成する。次に、ログイン情報２３２から端末ＩＤを抽出し、制御部２０７自身の記憶しているアプリ番号「００１」と抽出した端末ＩＤと生成した端末用精算画面データとを、送受信部２０１を介して管理サーバ６００へ送信する。

次に、管理サーバ６００から、アプリ番号「００１」と端末ＩＤと暗号化入力データを受信する。受信した暗号化入力データとサーバ共通鍵とを暗号処理部２０８へ出力し、復号を指示する。暗号処理部１０８から、入力データを受け取り、受け取った入力データを基に、利用者の出張費の精算処理を行う。

出張費の精算処理が終了すると、情報記憶部２１０から精算終了画面データを読み出し、読み出した精算終了画面データとログイン情報２３

２から、端末用精算終了画面データを生成し、アプリ番号「００１」とログイン情報２３２に含まれる端末ＩＤと生成した端末用精算終了画面データとを管理サーバ６００へ送信し、出張費精算のサービスを終了する。

（ii）パスワード変更

制御部２０７は、管理サーバ６００から、アプリサーバ２００と対応するアプリ番号とパスワード変更の対象となっている利用者が使用しているユーザ端末１００の端末ＩＤとユーザＩＤと暗号化現パスワードと暗号化新パスワードとパスワード変更の指示を受信すると、受信した端末ＩＤを一時的に記憶する。

次に、受信した暗号化現パスワードと暗号化新パスワードとサーバ共通鍵とを暗号処理部２０８へ出力し、復号を指示する。暗号処理部２０８から、現パスワードと新パスワードとを受け取り、受け取った現パスワードと受信したユーザＩＤとを含むパスワード情報２２３をパスワードテーブル２２１から選択する。次に選択したパスワード情報２２３のパスワードを、新パスワードに書き換える。

書き換えが正常に終了すると、制御部２０７は、終了信号「１」を生成する。ハードディスク不良などにより、書き換えが失敗すると、終了信号「０」を生成し、アプリサーバ２００自身のアプリ番号と一時的に記憶している端末ＩＤと生成した終了信号とを送受信部２０１を介して、管理サーバ６００へ送信し、パスワード変更の処理を終了する。

（iii）パスワード復旧処理

管理サーバ６００から、アプリサーバ２００と対応するアプリ番号と端末ＩＤとユーザＩＤと暗号化現パスワードと暗号化新パスワードとパスワード復旧の指示を受け取ると、端末ＩＤを一時的に記憶する。次に、制御部２０７は、受け取った暗号化現パスワードと暗号化新パスワードとサーバ共通鍵とを暗号処理部２０８へ出力し、復号を指示する。

暗号処理部２０８から、現パスワードと新パスワードとを受け取り、受け取った新パスワードと受信したユーザＩＤとを含むパスワード情報

２２３をパスワードテーブル２２１から選択する。選択したパスワード情報２２３に含まれるパスワードを受け取った現パスワードに書き換える。

パスワードの書き換えが正常に終了すると、終了信号「１」を生成する。パスワードの書き換えが失敗すると、終了信号「０」を生成する。次に、アプリサーバ２００自身と対応するアプリ番号と一時的に記憶した端末ＩＤと生成した終了信号とを送受信部２０１を介して、管理サーバ６００へ送信し、処理を終了する。

（iv）ログアウト処理

制御部２０７は、送受信部２０１を介して、管理サーバ６００から、アプリ番号とユーザ端末１００の端末ＩＤとログアウト通知を受信すると、アプリログインテーブル２３１内で受信した端末ＩＤを含むログイン情報２３２を探す。受信した端末ＩＤを含むログイン情報がアプリログインテーブル２３１内に存在しなければ、そのままログアウト処理を終了する。

受信した端末ＩＤを含むログイン情報２３２がアプリログインテーブル２３１内に存在すれば、受信した端末ＩＤを含むログイン情報２３２を削除し、ログアウト処理を終了する。

（５）認証部２０３

認証部２０３は、制御部２０７と外部機器との通信に先だって、秘密鍵２４２と公開鍵証明書２４３とを用いて外部機器との間で相互認証を行い、相互認証が成功した場合のみ制御部２０７と外部機器との通信を許可し、外部装置と同一のサーバ共通鍵を生成する。ここで、外部機器とは、具体的には、管理サーバ６００である。

（６）暗号処理部２０８

暗号処理部２０８は、制御部２０７から各種の情報とサーバ共通鍵を受け取り暗号化を指示される。暗号化の指示を受け取ると、受け取ったサーバ共通鍵を用いて受け取った情報に暗号化アルゴリズムＥ４を施し、暗号化情報を生成し、生成した暗号化情報を、制御部２０７へ出力する。

また、制御部２０７から各種の暗号化情報とサーバ共通鍵とを受け取り復号を指示される。復号の指示を受け取ると、受け取ったサーバ共通鍵を用いて、受け取った暗号化情報に復号アルゴリズムＤ３を施して、情報を生成し、生成した情報を制御部２０７へ出力する。

暗号処理部２０８が、制御部２０７から受け取る、暗号化情報は、具体的には、暗号化パスワード、暗号化入力データ、暗号化現パスワード及び暗号化新パスワードである。

ここで、復号アルゴリズムＤ３は、暗号化アルゴリズムＥ３により生成された暗号文を復号するアルゴリズムであり、暗号化アルゴリズムＥ３及びＥ４は、一例としてＤＥＳ暗号方式などの共通鍵暗号方式である。

１．４　管理サーバ６００

管理サーバ６００は、図１３に示すように、送受信部６０１、認証部６０３、パスワード変更部６０６、制御部６０７、暗号処理部６０８、パスワード復旧部６１４、変更判定部６０９、変更結果通知部６１５、情報記憶部６１０、入力部６１２及び表示部６１３から構成される。

管理サーバ６００は、具体的には図示されていないマイクロプロセッサ、ＲＡＭ、ＲＯＭ及びハードディスクから構成される。前記ＲＡＭ、ＲＯＭ及びハードディスクにはコンピュータプログラムが記憶されており、前記マイクロプロセッサが前記コンピュータプログラムに従って動作することにより、管理サーバ６００は、その機能を達成する。

（１）情報記憶部６１０

情報記憶部６１０は、ハードディスクユニットから構成され、一例として、図１４に示すように、パスワードテーブル６２１、ログインテーブル６３１ルーティングテーブル６４１、パスワード変更テーブル６５１、秘密鍵６６１、公開鍵証明書６６２、ＣＲＬ６６３及び認証局公開鍵６６４を記憶している。

パスワードテーブル６２１は、アプリサーバ２００の記憶しているパスワードテーブル２２１と同様の構成であるので、説明を省略する。

ログインテーブル６３１は、図１５に示すように、複数のログイン情

報６３２、６３３、６３４・・・から構成され、各ログイン情報は、ユーザＩＤ、氏名、パスワード、端末ＩＤ及び処理状況を含む。

ユーザＩＤは、管理サーバ６００によるパスワードの認証を終え、現在各種サービスを利用中の利用者と対応しており、氏名及びパスワードは、ユーザＩＤの示す利用者の氏名及びパスワードである。端末ＩＤは、ユーザＩＤの示す利用者が現在使用しているユーザ端末に固有の識別情報である。処理状況は、端末ＩＤの示すユーザ端末と管理サーバ６００及びアプリサーバ２００間で行っている処理の種類を示しており、パスワードの変更処理を行っているときは「パスワード変更中」、アプリサーバ２００による各種サービスに係る処理を行っているときは「通常」に設定されている。

ルーティングテーブル６４１は、図１６に示すように、複数のルート情報６４２、６４３・・・から構成され、各ルート情報は、アプリ番号、ホスト名、ＩＰアドレス及びポート番号を含む。

アプリ番号は、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄと対応しており、各アプリサーバが提供するサービスを示す識別情報である。これは、ユーザ端末１００が記憶しているアプリ番号表１２０に含まれるアプリ番号と同一のものである。ホスト名は、アプリ番号と対応するアプリサーバ２００を特定する識別情報である。ＩＰアドレスは、前記アプリサーバのネットワーク上の位置を示すＩＰアドレスであり、ポート番号は、管理サーバ６００が、アプリサーバ２００へ情報を送信する際に指定する送信先ポート番号である。

パスワード変更テーブル６５１は、図１７に示すように、複数の変更情報６５２、６５３、６５４・・・から構成される。各変更情報は、ユーザＩＤ、現行パスワード及び新パスワードを含む。

ユーザＩＤは、アプリサーバ２００及び管理サーバ６００の正当な利用者に割り当てられた識別情報である。現パスワードは、パスワード変更処理を行う時点で利用者が使用しているパスワードであり、新パスワードは、パスワード変更処理において、利用者が設定した新しいパスワ

ードである。具体的には、現パスワードは、図７の示すパスワード変更画面１９１内の空欄１９２に入力される文字列であり、新パスワードは、空欄１９３及び１９４に入力される文字列である。

公開鍵証明書６６２は、秘密鍵６６１と対になる公開鍵の正当性を証明するものであり、証明書ＩＤ、前記公開鍵及び認証局による署名データを含む。

ＣＲＬ６６３及び認証局公開鍵６６４は、ユーザ端末１００の記憶しているＣＲＬ１３７及び認証局公開鍵１３８と同一であるので説明を省略する。

また、情報記憶部６１０は、具体的には図示していないが、各種の画面データを記憶している。

（２）送受信部６０１

送受信部６０１は、ユーザ端末１００の端末ＩＤとユーザ端末１００のＩＰアドレスとを対応付けて記憶する。また、管理サーバ６００のＩＰアドレスを記憶している。

送受信部６０１は、管理サーバ６００内の各部と外部機器との間で情報の送受信を行う。

送受信部６０１が、送受信する各種情報は、一例として図４に示すパケット１４０の形体である。

送受信部６０１は、制御部６０７、パスワード変更部６０６又はパスワード復旧部６１４から、アプリ番号とユーザ端末１００の端末ＩＤと各種の情報からなるデータ部１４３を受け取り、送信を指示される。

制御部６０７から、ユーザ端末１００への送信を指示されると、送信元を管理サーバ６００のＩＰアドレスに設定し、端末ＩＤを基に送信先をユーザ端末１００のＩＰアドレスに設定し、受け取ったデータ部１４３を送信する。また、制御部６０７又はパスワード変更部６０６から情報を受け取り、アプリサーバ２００への送信を指示されると、アプリ番号を基にルーティングテーブル６４１からルート情報を選択し、選択したルート情報からＩＰアドレスとポート番号を抽出し、送信先アドレス

を抽出したＩＰアドレスに設定し、送信元を管理サーバ６００のＩＰアドレスに設定し、送信先ポート番号を抽出したポート番号に設定して送信する。

（３）入力部６１２及び表示部６１３

入力部６１２は、操作者による情報及び指示の入力を受け付け、受け付けた情報及び受け付けた指示に応じた操作指示情報を制御部６０７へ出力する。

表示部６１３は、制御部６０７からの指示により、各種情報を表示する。

（４）パスワード変更部６０６

パスワード変更部６０６は、制御部６０７から、アプリ番号と端末ＩＤとユーザＩＤと暗号化現パスワードと暗号化新パスワードとを受け取りパスワード変更を指示される。制御部６０７からパスワード変更を指示されると以下に説明するパスワード変更処理を行う。なお、以下の説明において、データ部１４３の生成については説明を省略し、単にアプリ番号、端末ＩＤ及び各種情報の出力と表現する。

（パスワード変更処理）

パスワード変更部６０６は、制御部６０７から、アプリ番号と端末ＩＤと暗号化現パスワードと暗号化新パスワードとを受け取りパスワード変更を指示されると、アプリサーバ２００に対してパスワードの変更を指示するパスワード変更指示を生成し、受け取ったユーザＩＤとアプリ番号とユーザＩＤと暗号化現パスワードと暗号化新パスワードと生成したパスワード変更指示とを送受信部６０１に出力し、アプリサーバ２００へ送信を指示する。

送信と同時に、パスワード変更部６０６は、アプリサーバ２００へパスワード変更指示を送信したことを示す変更指示送信済信号を生成し、生成した変更指示送信済信号と制御部６０７から受け取ったアプリ番号と端末ＩＤとを変更判定部６０９へ出力する。

（５）パスワード復旧部６１４

パスワード復旧部６１４は、制御部６０７からアプリ番号と端末ＩＤとユーザＩＤと暗号化現パスワードと暗号化新パスワードとを受け取りパスワード復旧を指示される。

また、変更判定部６０９からパスワード復旧指示の再送信を指示される。

制御部６０７からパスワード復旧を指示されると以下に説明するパスワード復旧処理を開始する。なお、以下の説明において、データ部１４３の生成については説明を省略し、単にアプリ番号、端末ＩＤ及び各種情報の出力と表現する。

（パスワード復旧処理）

パスワード復旧部６１４は、制御部６０７から、アプリ番号と端末ＩＤとユーザＩＤと暗号化現パスワードと暗号化新パスワードとを受け取りパスワード復旧を指示されると、アプリサーバ２００に対してパスワードを現パスワードに戻すことを指示するパスワード復旧指示を生成し、受け取ったアプリ番号と端末ＩＤと暗号化現パスワードと暗号化新パスワードと生成したパスワード復旧指示とを一時的に記憶する。次に、受け取ったアプリ番号と端末ＩＤと暗号化現パスワードと暗号化新パスワードと生成したパスワード復旧指示とを送受信部６０１へ出力し、アプリ番号と対応するアプリサーバ２００への送信を指示する。

送信と同時に、パスワード復旧部６１４は、アプリサーバ２００へパスワード復旧指示を送信したことを示す復旧送信済信号を生成し、生成した復旧送信済信号と記憶しているアプリ番号と端末ＩＤとを変更判定部６０９へ出力する。

変更判定部６０９から、パスワード復旧指示の再送信を指示されると、パスワード復旧部６１４は、記憶しているアプリ番号と端末ＩＤと暗号化現パスワードと暗号化新パスワードとパスワード復旧指示とを読み出し、読み出したアプリ番号と端末ＩＤと暗号化現パスワードと暗号化新パスワードとパスワード復旧指示とを送受信部６０１を介して再送信する。

再送信と同時に、復旧送信済信号を変更判定部６０９へ出力する。

（６）変更判定部６０９

変更判定部６０９は、時間の経過に伴って経過時間を計測するｔｉｍｅカウンタとパスワード復旧指示の送信回数を数える回数カウンタとを備える。

また、変更判定部６０９は、あらかじめ、最大待ち時間と制限回数を記憶している。最大待ち時間は、パスワード変更部６０６又はパスワード復旧部６１４がパスワード変更指示又はパスワード復旧指示を送信してから終了信号を受け取るまでの待機時間の上限値「１秒」である。パスワード変更指示を送信してから最大待ち時間を超えて終了信号を受信しなければ、パスワードの変更失敗を示す変更終了信号「０」を生成する。パスワード復旧指示を送信してから、最大待ち時間を超えて終了信号を受信しなければ、パスワード復旧部６１４にパスワード復旧指示の再送信を指示する。

制限回数は、１台のアプリサーバ２００へパスワード復旧指示を送信できる回数の最大値「３回」である。パスワード復旧指示の送信回数が「３回」を超えると、パスワード復旧の失敗を示す復旧終了信号「０」を生成する。

変更判定部６０９は、パスワード変更部６０６から変更指示送信済信号とアプリ番号と端末ＩＤとを受け取る。

変更判定部６０９は、パスワード復旧部６１４から、復旧指示送信済信号とアプリ番号と端末ＩＤとを受け取る。また、パスワード復旧部６１４から復旧指示送信済信号のみを受け取る。

以下に変更判定部６０９の行う（ｉ）パスワード変更の判定処理と(ii)パスワード復旧の判定処理について説明する。

（ｉ）パスワード変更の判定処理

変更判定部６０９は、パスワード変更部６０６から変更指示送信済信号とアプリ番号と端末ＩＤとを受け取ると、受け取ったアプリ番号と端末ＩＤとを内部に一時的に記憶する。

また、変更指示送信済信号を受け取ると同時に、ｔｉｍｅカウンタを０に初期化し、経過時間の計測を開始する。

次に、送受信部６０１を介してアプリサーバ２００から終了信号を受信すると、受信した終了信号を判別し、終了信号が「１」であれば、アプリサーバ２００のパスワード変更が成功であることを示す変更終了信号「１」を生成する。受信した終了信号が「０」であると判断すると、アプリサーバ２００のパスワード変更が失敗であることを示す変更終了信号「０」を生成する。

また、アプリサーバ２００から終了信号を受信していない場合、ｔｉｍｅカウンタの値と最大待ち時間とを比較する。ｔｉｍｅカウンタが最大待ち時間を超えていないと判断すると、終了信号を受信するかｔｉｍｅカウンタが最大待ち時間を超えるまで、ｔｉｍｅカウンタと最大待ち時間の比較を繰り返す。

ｔｉｍｅカウンタの値が最大時間を超えていると判断すると、変更判定部６０９は、アプリサーバ２００のパスワード変更が失敗であると判断し、変更終了信号「０」を生成する。

次に、記憶しているアプリ番号と端末ＩＤと生成した変更終了信号とを、制御部６０７へ出力する。

（ii）パスワード復旧の判定処理

変更判定部６０９は、パスワード復旧部６１４から、復旧指示送信済信号とアプリ番号と端末ＩＤとを受け取ると、受け取ったアプリ番号と端末ＩＤとを内部に一時的に記憶し、回数カウンタを０に初期化する。

また、復旧指示送信済信を受け取ると同時に、パスワード変更部６０６は、ｔｉｍｅカウンタを０に初期化して経過時間の計測を開始する。

パスワード復旧部６１４から、復旧指示送信済信号のみを受け取ると、回数カウンタの初期化は行わず、ｔｉｍｅカウンタを０に初期化して経過時間の計測を開始する。

次に、送受信部６０１を介して、アプリサーバ２００からの終了信号を受信すると、受信した終了信号を判別し、終了信号が「１」であれば、

アプリサーバ２００のパスワード復旧が成功であることを示す復旧終了信号「１」を生成する。

受信した終了信号が「０」であると判断すると、回数カウンタに１加算する。次に回数カウンタの値と制限回数とを比較する。回数カウンタが制限回数を超えていないと判断すると、パスワード復旧部６１４にパスワード復旧指示の再送信を指示する。

また、アプリサーバ２００からの終了信号を受信していない場合、ｔｉｍｅカウンタと最大待ち時間とを比較する。ｔｉｍｅカウンタが最大待ち時間を超えていないと判断すると、終了信号を受信するか経過時間が最大待ち時間を超えるまで、ｔｉｍｅカウンタと最大待ち時間の比較を繰り返す。

ｔｉｍｅカウンタが、最大待ち時間を超えていると判断すると、回数カウンタに１加算する。次に、回数カウンタと制限回数を比較する。回数カウンタが、制限回数以内であれば、パスワード復旧部６１４にパスワード復旧指示の再送信を指示する。

回数カウンタが、制限回数を超えていると判断すると、パスワード復旧が失敗であることを示す復旧終了信号「０」を生成する。

復旧終了信号を生成すると、次に、記憶しているアプリ番号と端末ＩＤと生成した復旧終了信号とを制御部６０７へ出力する。

（７）制御部６０７

制御部６０７は、上記のプロセッサがコンピュータプログラムに従って動作することにより、管理サーバ６００で実行する各種の情報処理を制御する。

制御部６０７は、アプリサーバ２００とアプリサーバ２００が提供するサービスを示すアプリ番号とを対応付けて記憶している。

制御部６０７は、送受信部６０１を介してユーザ端末１００から公開鍵証明書を受信する。

ユーザ端末１００から公開鍵証明書を受信すると、受信した公開鍵証明書を認証部６０３へ出力し、相互認証を指示する。認証部６０３によ

る相互認証が終了し、端末共通鍵を受け取る。受け取った端末共通鍵を用いて秘密通信をすることにより、ユーザ端末１００との間で以下に説明する処理を安全に行う。

また、制御部６０７が、送受信部６０１を介して送受信する情報は、図４に示すようなパケット１４０の形体である。制御部６０７は、受信したアプリ番号を判別し、利用者が利用しようとするサービスを提供する機器がアプリサーバ２００又は管理サーバ６００のいずれであるかを判断する。制御部６０７は、各種情報を送信する際、送信する情報と処理の対象となっている利用者の使用しているユーザ端末１００の端末ＩＤと処理を実行する機器と対応するアプリ番号からなるデータ部１４３を生成し、生成したデータ部１４３を送受信部６０１へ出力し、送信を指示する。ここで、処理を実行する機器とは、アプリサーバ２００及び管理サーバ６００である。

以下に説明する制御部６０７の行う処理において、上記のようなデータ部１４３の生成に関する説明は省略し、単にアプリ番号と端末ＩＤと各種情報と表現する。

制御部６０７は、利用者のログイン処理、各種サービスの中継処理、パスワード変更制御、パスワード復旧制御及びログアウト処理を行う。以下に、利用者のログイン処理、各種サービスの中継処理、パスワード変更制御、パスワード復旧制御及びログアウト処理について説明する。

（ｉ）利用者のログイン処理

制御部６０７は、認証部６０３による、相互認証が終了すると、認証部６０３から端末共通鍵を受け取り、受け取った端末共通鍵を記憶する。制御部６０７は、情報記憶部６１０からログイン画面データを読み出し、送受信部６０１を介して読み出したログイン画面データをユーザ端末１００へ送信する。

次に、ユーザ端末１００からアプリ番号「００５」と端末ＩＤとユーザＩＤと暗号化パスワードとを受信し、受信した暗号化パスワードと端末共通鍵とを暗号処理部６０８に出力し、復号を指示する。暗号処理部

６０８からパスワードを受け取ると、パスワードテーブル６２１内で、受信したユーザＩＤと受け取ったパスワードを含むパスワード情報を検索する。受信したユーザＩＤと受け取ったパスワードを含むパスワード情報が存在しないと判断すると、再度、ログイン画面データをユーザ端末１００へ送信する。

受信したユーザＩＤと受け取ったパスワードを含むパスワード情報が存在すると判断すると、受信したユーザＩＤと受け取ったパスワードを含むパスワード情報を選択する。受信した端末ＩＤと選択したパスワード情報とを基に、ログイン情報６３２を生成し、生成したログイン情報６３２をログインテーブル６３１に追加して書き込む。このとき、処理状況は「通常」に設定する。これにより、ログイン処理完了と判断する。

これ以降の処理において、ユーザ端末１００から各種情報を受信するたびに、各種情報と供に受信する端末ＩＤを含むログイン情報６３２がログインテーブル６３１内に存在することを確認し、ユーザ端末１００の利用者がログイン済みであることを確認する。以下の説明において、ログイン済みの確認については、詳細な説明を省略する。

次に、情報記憶部６１０からメニュー画面データを読み出し、読み出したメニュー画像データと書き込んだログイン情報６３２に含まれるユーザＩＤ及び氏名を基に、端末用メニュー画面データを生成し、生成した端末用メニュー画面データを送受信部６０１を介して、ユーザ端末１００へ送信する。次に、送受信部６０１を介して、ユーザ端末１００からアプリ番号と端末ＩＤとサービス開始要求又はアプリ番号と端末ＩＤとパスワード変更指示を受信する。アプリ番号と端末ＩＤとサービス開始要求を受信するとユーザ端末１００とアプリサーバ２００との中継処理を行い、アプリ番号と端末ＩＤとパスワード変更指示を受信するとパスワード変更処理及びパスワード復旧処理を行う。

（ii）各種サービスの中継処理

制御部６０７は、アプリ番号と端末ＩＤサービス開始要求を受信すると、以下に説明する手順で、受信したアプリ番号の示すアプリサーバ２

００とユーザ端末１００との間で中継処理を行う。

ここでは、第１アプリサーバ２００ａとユーザ端末１００との間の中継処理について説明する。

制御部６０７は、ユーザ端末１００の利用者がログイン済みであることを確認し、認証部６０３へアプリサーバ２００ａとの相互認証を指示する。認証部６０３による相互認証が終了し、認証部６０３からサーバ共通鍵を受け取り、受け取ったサーバ共通鍵を記憶する。

次に、ログインテーブル６３１内で受信した端末ＩＤ含むログイン情報６３２を選択し、選択したログイン情報６３２からユーザＩＤとパスワードを抽出する。抽出したパスワードとサーバ共通鍵とを暗号処理部６０８へ出力し、パスワードの暗号化を指示する。次に、暗号処理部６０８から暗号化パスワードを受け取る。ユーザ端末１００から受信したアプリ番号「００１」と端末ＩＤとサービス開始要求と読み出したユーザＩＤと暗号処理部６０８から受け取った暗号化パスワードとを、送受信部６０１へ出力し、第１アプリサーバ２００ａへの送信を指示する。

次に、制御部６０７は、送受信部６０１を介して、アプリサーバ２００ａからアプリ番号「００１」と端末ＩＤとパスワードエラー信号とユーザＩＤ又はアプリ番号「００１」と端末ＩＤと端末用精算画面データを受信する。

アプリ番号「００１」と端末ＩＤとパスワードエラー信号とユーザＩＤとを受信すると、制御部６０７は、情報記憶部６１０から強制終了画面データ読み出す。次に受信したユーザＩＤを含むログイン情報６３２からユーザＩＤと氏名を抽出する。

読み出した強制終了画面データと抽出したユーザＩＤと氏名とを基に、端末用強制終了画面データを生成し、送受信部６０１を介して、受信した端末ＩＤと生成した端末用強制終了画面データをユーザ端末１００へ送信する。次に、受信したユーザＩＤとエラー画面データとから、エラー画面３３１を生成し、表示部６１３へ出力し、パスワードの不一致が発生していることを管理サーバ６００の操作者に通知する。

アプリ番号「００１」と端末ＩＤと端末用精算画面データとを受信すると、送受信部６０１を介して、受信したアプリ番号「００１」と端末ＩＤと端末用精算画面データとをユーザ端末１００へ送信する。

次に、送受信部６０１を介して、ユーザ端末１００から、アプリ番号「００１」、端末ＩＤ及び暗号化入力データを受信する。受信した端末ＩＤを基に、ユーザ端末１００の利用者がログイン済みであることを確認する。

次に、受信した暗号化入力データと端末共通鍵とを暗号処理部６０８へ出力し、暗号化入力データの復号を指示する。暗号処理部６０８から入力データを受け取る。次に、受け取った入力データとサーバ共通鍵とを暗号処理部６０８へ出力し、入力データの暗号化を指示する。暗号処理部６０８から暗号化入力データを受け取る。

次に、制御部６０７は、アプリ番号「００１」と受信した端末ＩＤと暗号処理部６０８から受け取った暗号化入力データとを送受信部６０１を介して、第１アプリサーバ２００ａへ送信する。

次に、送受信部６０１を介して、アプリサーバ２００ａから、アプリ番号「００１」、端末ＩＤ及び端末用精算終了画面データを受信する。受信したアプリ番号「００１」、端末ＩＤ及び端末用精算終了画面データをユーザ端末１００へ送信する。

（iii）パスワード変更制御

制御部６０７は、受付処理、パスワード変更指示、結果通知の順序でパスワード変更制御を行う。以下に、受付処理、パスワード変更指示及び結果通知の処理について説明する。

（iii－ａ）受付処理

制御部６０７は、送受信部６０１を介して、ユーザ端末１００からアプリ番号「００５」と端末ＩＤとパスワード変更指示とを受信する。次に、ユーザ端末１００の利用者がログイン済みであることを確認する。次に、情報記憶部６１０からパスワード変更画面データを読み出し、読み出したパスワード変更画面データとログイン情報６３２とを基に、

端末用パスワード変更画面データを生成し、生成した端末用パスワード変更画面データを送受信部６０１を介して、ユーザ端末１００へ送信する。

次に、送受信部６０１を介して、ユーザ端末１００からアプリ番号「００５」と端末ＩＤと暗号化現パスワードと暗号化新パスワードとを受信する。制御部６０７は、受信した端末ＩＤを含む、ログイン情報６３２を選択し、選択したログイン情報６３２の処理状況を「パスワード変更中」に書き換える。

次に、受信した暗号化現パスワードと暗号化新パスワードと端末共通鍵とを暗号処理部６０８へ出力し、暗号化現パスワードと暗号化新パスワードの復号を指示する。暗号処理部６０８から、生成された現パスワードと新パスワードとを受け取る。

次に、書き換えたログイン情報６３２からユーザＩＤを読み出し、パスワードテーブル６２１上で、読み出したユーザＩＤと受け取った現パスワードとを含むパスワード情報の有無を確認する。読み出したユーザＩＤと受け取った現パスワードとを含むパスワード情報が存在しないと判断すると、送受信部６０１を介して、ユーザ端末１００へパスワード変更画面を再度送信し、現パスワードと新パスワードの再入力を促す。

パスワードテーブル６２１上に、読み出したユーザＩＤと受け取った現パスワードとを含むパスワード情報が存在すると判断すると、次に、読み出したユーザＩＤを含むパスワード変更情報６５２をパスワード変更テーブル６５１から選択する。選択したパスワード変更情報６５２に含まれる現パスワードを暗号処理部６０８から受け取った現パスワードに書き換え、選択したパスワード変更情報に含まれる新パスワードを暗号処理部６０８から受け取った新パスワードに書き換える。

（iii－ｂ）パスワード変更処理

次に、制御部６０７は、以下に説明する手順で第１アプリサーバ２００ａ～第４アプリサーバ２００ｄのパスワード変更を行う。

制御部６０７は、認証部６０３へ、第１アプリサーバ２００ａとの相

互認証を指示する。認証部６０３による相互認証が終了し、認証部６０３からサーバ共通鍵を受け取り記憶する。次に、パスワード変更情報６５２から現パスワードと新パスワードとを抽出し、抽出した現パスワードと新パスワードと第１アプリサーバ２００ａとの相互認証により生成されたサーバ共通鍵とを暗号処理部６０８へ出力し、現パスワードと新パスワードの暗号化を指示する。

次に、暗号処理部６０８から暗号化現パスワードと暗号化新パスワードとを受け取る。パスワード変更情報６５２からユーザＩＤを抽出する。次に、制御部６０７は、第１アプリサーバ２００ａと対応するアプリ番号「００１」とユーザ端末１００の端末ＩＤと抽出したユーザＩＤと受け取った暗号化現パスワードと暗号化新パスワードとをパスワード変更部６０６へ出力しパスワード変更を指示する。

次に、変更判定部６０９からアプリ番号「００１」と端末ＩＤと変更終了信号を受け取る。受け取った変更終了信号がパスワード変更成功を示す「１」であれば第１アプリサーバ２００ａのパスワード変更が成功であると判断する。

受け取った変更終了信号が「０」であると判断すると、第１アプリサーバ２００ａのパスワード変更が失敗であると判断し、第２アプリサーバ２００ｂ以降のパスワード変更を中止し、パスワード復旧制御へ処理を移す。

第１アプリサーバ２００ａのパスワード変更が成功であると判断すると、同様にして、相互認証、現パスワードと新パスワードの暗号化、パスワード変更の指示及び変更終了信号の取得の手順で第２アプリサーバ２００ｂのパスワード変更を行う。

第２アプリサーバ２００ｂのパスワード変更が成功であれば、同様にして第３アプリサーバ２００ｃのパスワード変更を行い、失敗であれば、第３アプリサーバ２００ｃ及び第４アプリサーバ２００ｄのパスワード変更を中止し、パスワード復旧処理へ移る。

第３アプリサーバ２００ｃのパスワード変更が成功であれば、続いて

第４アプリサーバ２００ｄのパスワード変更を行い、失敗であれば、第４アプリサーバ２００ｄのパスワード変更を中止し、パスワード復旧処理に移る。

第４アプリサーバ２００ｄのパスワード変更が成功であれば、以下の結果通知を行い、失敗であれば、パスワード復旧処理を行う。

（iii－ｃ）結果通知

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄのパスワード変更が全て成功すると、制御部６０７は、情報記憶部６１０の記憶しているパスワードテーブル６２１内において、パスワード変更部６０６へ出力したユーザＩＤを含むパスワード情報を選択し、選択したパスワード情報に含まれるパスワードを、新パスワードに書き換える。次に、ログインテーブル６３１から、出力したユーザＩＤを含むログイン情報６３２を選択し、選択したログイン情報６３２に含まれるパスワードを新パスワードに書き換える。

次に、パスワード変更の完了を示す完了信号を生成し、書き換えたログイン情報６３２からユーザＩＤと氏名とを抽出し、変更結果通知部６１５に生成した完了信号とユーザＩＤと端末ＩＤとを出力し、ユーザ端末１００への結果通知を指示する。

次に、ログイン情報６３２の処理状況を「通常」に書き換える。

（iv）パスワード復旧処理

上記の（iii）において説明したパスワード変更処理の途中で何れかのアプリサーバ２００のパスワード変更が失敗すると、制御部６０７は、パスワード復旧の処理を行う。

具体的には、制御部６０７は、変更判定部６０９から変更終了信号「０」と供に受け取ったアプリ番号により、パスワード変更が失敗したアプリサーバ２００を判別する。第１アプリサーバ２００ａ～第３アプリサーバ２００ｃのパスワード変更処理は成功し、第４アプリサーバ２００ｄのパスワード変更処理が失敗であると判断すると、第３アプリサーバ２００ｃ～第１アプリサーバ２００ａの順にアプリサーバのパスワード復

旧処理を行い、次に、失敗通知処理を行う。

第１アプリサーバ２００ａと第２アプリサーバ２００ｂのパスワード変更処理は成功し、第３アプリサーバ２００ｃのパスワード変更処理が失敗であると判断すると、第２アプリサーバ２００ｂ～第１アプリサーバ２００ａの順にアプリサーバのパスワード復旧処理を行い、次に、失敗通知処理を行う。

第１アプリサーバ２００ａのパスワード変更処理は成功し、第２アプリサーバ２００ｃのパスワード変更処理が失敗であると判断すると、第１アプリサーバ２００ａにアプリサーバのパスワード復旧処理を行い、次に、失敗通知処理を行う。

第１アプリサーバ２００ａのパスワード変更処理が失敗であると判断すると、失敗通知処理のみを行う。

また、何れかのアプリサーバ２００において、アプリサーバのパスワード復旧処理が失敗すると、エラー処理を行う。

以下に、アプリサーバのパスワード復旧処理、失敗通知処理及びエラー処理の詳細を説明する。

（ⅳ－ａ）アプリサーバのパスワード復旧処理

制御部６０７は、パスワード変更情報６５２から現パスワードと新パスワードとを抽出し、抽出した現パスワードと新パスワードと該当するアプリサーバ２００のサーバ共通鍵とを暗号処理部６０８に出力し、現パスワードと新パスワードとの暗号化を指示する。暗号処理部６０８から、暗号化現パスワードと暗号化新パスワードとを受け取り、アプリサーバ２００に対応するアプリ番号とユーザ端末１００の端末ＩＤとパスワード変更情報６５２に含まれるユーザＩＤと受け取った暗号化現パスワードと暗号化新パスワードとにとをパスワード変更部６０６へ出力し、パスワード復旧を指示する。

次に、パスワード変更部６０６からアプリ番号と端末ＩＤと復旧終了信号とを受け取る。受け取った復旧終了信号がパスワード復旧の成功を示す「１」であれば、受け取ったアプリ番号と対応するアプリサーバ２

００のパスワード復旧が成功であると判断し、次のアプリサーバ２００のパスワード復旧又は失敗通知処理を行う。

受け取った復旧終了信号がパスワード復旧失敗を示す「０」であると、該当するアプリサーバ２００のパスワード復旧が失敗であると判断する。

アプリサーバ２００のパスワード復旧が失敗であると判断すると、他のアプリサーバ２００の復旧処理及び失敗通知の処理を行わず、後述するエラー処理を行う。

（ⅳ－ｂ）失敗通知処理

制御部６０７は、パスワード復旧の失敗を示す失敗信号を生成し、変更判定部６０９から受け取った端末ＩＤを含むログイン情報６３２を選択し、選択したログイン情報６３２からユーザＩＤと氏名を抽出し、生成した失敗信号と抽出したユーザＩＤと氏名とを変更結果通知部６１５へ出力し、結果通知を指示する。

次に、ログイン情報６３２の処理状況を「通常」に書き換え処理を終了する。

（ⅳ－ｃ）エラー処理

アプリサーバ２００何れかのパスワード復旧の処理が失敗であると判断すると、制御部６０７は、情報記憶部６１０から強制終了画面データを読み出し、読み出した強制終了画面データとログイン情報６３２に含まれるユーザＩＤと氏名を基に端末用強制終了画面データを生成し、生成した端末用強制終了画面データを、送受信部６０１を介して、ユーザ端末１００へ送信する。

次に、情報記憶部６１０からエラー画面データを読み出し、読み出したエラー画面データとログイン情報６３２に含まれるユーザＩＤからエラー画面３３１を生成し、生成したエラー画面３３１を表示部６１３に表示し、操作者にエラー発生を通知する。図１８は、ここで表示されるエラー画面３３１の一例である。

（ｖ）ログアウト処理

制御部６０７は、ユーザ端末１００から、送受信部６０１を介して、

アプリ番号「００５」と端末ＩＤとログアウト通知とを受信する。ログアウト通知を受信すると、受信した端末ＩＤとログアウト通知とを、送受信部６０１を介して第１アプリサーバ２００ａ～第４アプリサーバ２００ｄへ送信する。次に、受信した端末ＩＤを含むログイン情報６３２をログインテーブル６３１から削除する。

（８）変更結果通知部６１５

変更結果通知部６１５は、制御部６０７から完了信号とユーザＩＤと端末ＩＤと結果通知の指示を受け取る。

また、制御部６０７から失敗信号とユーザＩＤと氏名と結果通知の指示を受け取る。

完了信号とユーザＩＤと端末ＩＤと結果通知の指示を受け取ると、変更結果通知部６１５は、情報記憶部６１０から変更完了画面データを読み出し、読み出した変更完了画面データと受け取ったユーザＩＤと氏名とを基に、端末用変更完了画面データを生成し、生成した端末用変更完了画面データをユーザ端末１００へ送信する。

失敗信号とユーザＩＤと端末ＩＤと結果通知の指示を受け取ると、変更結果通知部６１５は、情報記憶部６１０から変更失敗画面データを読み出し、読み出した更失敗画面データと、受け取ったユーザＩＤと氏名を基に、端末用変更失敗画面データを生成し、生成した端末用変更失敗画面データを送受信部６０１を介して、ユーザ端末１００へ送信する。

（９）認証部６０３

認証部６０３は、制御部６０７の指示によりインターネット２０と接続されている外部機器と相互認証を行い共通鍵を生成する。

ここで、外部装置とはユーザ端末１００及びアプリサーバ２００であり、ユーザ端末１００との間では、端末共通鍵を共有し、各アプリサーバ２００との間では、それぞれのアプリサーバとサーバ共通鍵を共有する。

（１０）暗号処理部６０８

暗号処理部６０８は、制御部６０７からの指示により各種情報の暗号

化及び復号を行う。

具体的には、制御部６０７から、暗号化パスワードと端末共通鍵、暗号化入力データと端末共通鍵又は暗号化現パスワードと暗号化新パスワードと端末共通鍵とを受け取る。受け取った端末共通鍵を用いて受け取った暗号化パスワード、暗号化入力データ、暗号化現パスワード及び暗号化新パスワードに復号アルゴリズムＤ１を施して、パスワードを生成し、生成したパスワードを制御部６０７へ出力する。

また、パスワードとサーバ共通鍵、入力データとサーバ共通鍵又は現パスワードと新パスワードとサーバ共通鍵とを受け取る。受け取ったサーバ共通鍵を用いて、受け取ったパスワード、入力データ、現パスワード及び新パスワードに暗号化アルゴリズムＥ３を施して暗号化パスワード、暗号化入力データ、暗号化現パスワード及び暗号化新パスワードを生成し、生成した暗号化パスワード、暗号化入力データ、暗号化現パスワード及び暗号化新パスワードを制御部６０７へ出力する。

１．５パスワード変更システムの動作

パスワード変更システムの動作について以下に説明する。

（１）ユーザ端末１００による処理

ユーザ端末１００による処理について図１９～図２６に示すフローチャートを用いて説明する。なお、具体的には図示していないが、以下の動作において、機器間の各種情報の送受信の際には、処理を実行するアプリサーバ２００又は管理サーバ６００のアプリ番号とユーザ端末１００の端末ＩＤが各種情報と供に送受信される。

ユーザ端末１００は、利用者のボタン操作を受け付け（ステップＳ１０１）、電子申請を示すボタン操作を受け付けると、ステップＳ１０２へ処理を移す。その他の処理を示すボタン操作を受け付けると、その他の処理を行う（ステップＳ１００）。

ユーザ端末１００は、管理サーバ６００と相互認証を行い端末共通鍵を共有する（ステップＳ１０２）。

ユーザ端末１００との相互認証が完了すると、管理サーバ６００は、

ログイン画面データを読み出し（ステップＳ１０３）、読み出したログイン画面データを、ユーザ端末１００へ送信する（ステップＳ１０４）。

ユーザ端末１００は、管理サーバ６００からログイン画面データを受信し、受信したログイン画面データからログイン画面１５１を生成しモニタに表示する（ステップＳ１０５）。次に、利用者によるユーザＩＤとパスワードの入力を受け付け（ステップＳ１０７）、受け付けたパスワードを、端末共通鍵を用いて暗号化し暗号化パスワードを生成する（ステップＳ１０８）。ユーザＩＤと生成した暗号化パスワードとを、インターネット２０を介して管理サーバ６００へ送信する（ステップＳ１０９）。

管理サーバ６００は、インターネット２０を介してユーザＩＤと暗号化パスワードとを受け取り、受け取った暗号化パスワードを端末共通鍵を用いて復号し、パスワードを生成する（ステップＳ１１１）。次に、パスワードテーブル６２１内で受け取ったユーザＩＤとパスワードを含むパスワード情報の有無を確認し（ステップＳ１１２）、受け取ったユーザＩＤとパスワードを含むパスワード情報が存在しなければ、認証失敗と判断し（ステップＳ１１３のＮＯ）、ステップＳ１０３から処理をやり直す。受け取ったユーザＩＤとパスワードを含むパスワード情報が存在すれば、認証成功と判断し（ステップＳ１１３のＹＥＳ）、受け取ったユーザＩＤとパスワードを含むパスワード情報と受信したユーザ端末１００の端末ＩＤとを基に、ログイン情報６３２を生成しログインテーブル６３１に追加して書き込む（ステップＳ１１５）。

次に、情報記憶部６１０からメニュー画面データを読み出し、読み出したメニュー画面データと、ログインテーブル６３１に追加したログイン情報６３２とを基に端末用メニュー画面データを生成し（ステップＳ１１６）、生成した端末用メニュー画面データをインターネット２０を介して、ユーザ端末１００へ送信する（ステップＳ１１７）。

ユーザ端末１００は、インターネット２０を介して端末用メニュー画面データを受信し、受信した端末用メニュー画面データからメニュー画面１６１を生成し、モニタに表示する（ステップＳ１２１）。次に、利用

者によるメニューの選択を受け付ける（ステップＳ１２２）。

利用者のボタン操作により、パスワード変更が選択されると（ステップＳ１２２）、パスワード変更処理へ移行する（ステップＳ１２７）。

利用者により、出張費精算が選択されると（ステップＳ１２２）、アプリ番号「００１」を読み出す（ステップＳ１２３）。利用者により、休暇申請が選択されると（ステップＳ１２２）、アプリ番号「００２」を読み出す（ステップＳ１２４）。利用者により、会議室予約が選択されると（ステップＳ１２２）、アプリ番号「００３」を読み出す（ステップＳ１２５）。利用者により、従業員購入が選択されると（ステップＳ１２２）、アプリ番号「００４」を読み出す（ステップＳ１２６）。次に、読み出したアプリ番号とサービス開始要求を管理サーバ６００へ送信する（ステップＳ１２８）。

管理サーバ６００は、インターネット２０を介してユーザ端末１００からアプリ番号とサービス開始要求とを受信する。サービス開始要求とともに受信した端末ＩＤを含むログイン情報６３２を選択し、選択したログイン情報６３２に含まれる処理状況が「通常」であるか否かを確認する（ステップＳ１３１）。処理状況が「通常」でないと判断すると（ステップＳ１３１のＮＯ）、情報記憶部６１０からｗａｉｔメッセージを読み出し（ステップＳ１４６）、読み出したｗａｉｔメッセージを、インターネット２０を介してユーザ端末１００へ送信する（ステップＳ１４７）。

ユーザ端末１００は、管理サーバ６００から、ｗａｉｔメッセージを受信し、受信したｗａｉｔメッセージを表示する（ステップＳ１４８）。

選択したログイン情報６３２の処理状況が「通常」であると判断すると（ステップＳ１３１のＹＥＳ）、次に、受信したアプリ番号を判別し（ステップＳ１３２）、アプリ番号が「００２」であると判断すると（ステップＳ１３２の００２）、第２アプリサーバ２００ｂとの通信を開始する。アプリ番号が「００３」であると判断すると（ステップＳ１３２の００３）、第３アプリサーバ２００ｃとの通信を開始する。アプリ番号が「００４」であると判断すると（ステップＳ１３２の００４）、第４アプリサ

ーバ２００ｄとの通信を開始する（ステップＳ１３５）。

アプリ番号が「００１」であると判断すると（ステップＳ１３２の００１）、第１アプリサーバ２００ａとの通信を開始する。先ず、管理サーバ６００は、第１アプリサーバ２００ａと相互認証を行いサーバ共通鍵を共有する（ステップＳ１３６）。

次に、選択したログイン情報６３２に含まれるユーザＩＤとパスワードを読み出し（ステップＳ１３９）、読み出したパスワードをサーバ共通鍵を用いて暗号化して、暗号化パスワードを生成する（ステップＳ１４１）。受信したサービス開始要求とアプリ番号「００１」と読み出したユーザＩＤと生成した暗号化パスワードとを第１アプリサーバ２００ａへ送信する（ステップＳ１４２）。

第１アプリサーバ２００ａは、インターネット２０を介して管理サーバ６００から、サービス開始要求とアプリ番号「００１」とユーザＩＤと暗号化パスワードとを受信し、サーバ共通鍵を用いて、受信した暗号化パスワードを復号しパスワードを生成する（ステップＳ１５１）。パスワードテーブル２２１内で、受信したユーザＩＤと生成したパスワードとを含むパスワード情報の有無を確認し（ステップＳ１５２）、受信したユーザＩＤと生成したパスワードとを含むパスワード情報が存在しなければ、認証失敗と判断し（ステップＳ１５３のＮＯ）、管理サーバ６００の記憶しているパスワードと第１アプリサーバ２００ａの記憶しているパスワードとが一致していないことを示すパスワードエラー信号と、受信したユーザＩＤとをインターネット２０を介して管理サーバ６００へ送信する（ステップＳ１６６）。

管理サーバ６００は、第１アプリサーバ２００ａからパスワードエラー信号とユーザＩＤとを受信し、端末用強制終了画面データを生成し（ステップＳ１６７）、生成した端末用強制終了画面データをユーザ端末１００へ送信する（ステップＳ１６８）。次に、管理サーバ６００は、エラー画面３３１を生成し（ステップＳ１６９）、生成したエラー画面を表示部６１３へ表示しパスワードの不一致の発生を操作者に知らせる（ステッ

プＳ１７１）。

ユーザ端末１００は、インターネット２０を介して、管理サーバ６００から端末用強制終了画面データを受信し、受信した端末用強制終了画面データから強制終了画面３２１を生成し、生成した強制終了画面３２１をモニタに表示し（ステップＳ１７２）、処理を終了する。

パスワードテーブル２２１内に、受信したユーザＩＤと生成したパスワードとを含むパスワード情報２２３が存在すると、第１アプリサーバ２００ａは、認証成功と判断し（ステップＳ１５３のＹＥＳ）、パスワード情報２２３とサービス開始要求と供に受信した端末ＩＤとを基に、ログイン情報２３２を生成し、生成したログイン情報２３２をアプリログインテーブル２３１に追加して書き込む（ステップＳ１５４）。

次に、第１アプリサーバ２００ａは、端末用精算画面データを生成し（ステップＳ１５５）、生成した端末用精算画面データを管理サーバ６００へ送信する（ステップＳ１５６）。

管理サーバ６００は、インターネット２０を介して、第１アプリサーバ２００ａから端末用精算画面データを受信し、受信した端末用精算画面データをユーザ端末１００へ送信する（ステップＳ１５８）。

ユーザ端末１００は、インターネット２０を介して、管理サーバ６００から端末用精算画面データを受信し、受信した端末用精算画面データから精算画面１７１を生成し、モニタに表示する（ステップＳ１５９）。次に、利用者によるデータの入力を受け付け（ステップＳ１６１）、端末共通鍵を用いて受け付けた入力データを暗号化し、暗号化入力データを生成する（ステップＳ１６２）。次に、生成した暗号化入力データを、管理サーバ６００へ送信する（ステップＳ１７６）。

管理サーバ６００は、インターネット２０を介して、ユーザ端末１００から暗号化入力データを受信し（ステップＳ１７７）、受信した暗号化入力データを端末共通鍵を用いて復号し、入力データを生成する（ステップＳ１７７）。次に、サーバ共通鍵を用いて、生成した入力データを暗号化して暗号化入力データを生成し（ステップＳ１７９）、生成した暗号

化入力データを第１アプリサーバ２００ａへ送信する(ステップＳ１８１)。

第１アプリサーバ２００ａは、インターネット２０を介して暗号化入力データを受信し、サーバ共通鍵を用いて受信した暗号化入力データを復号し、入力データを生成する（ステップＳ１８２)。次に、生成した入力データを基に、出張費精算処理を行う（ステップＳ１８３)。出張費精算処理が終わると、第１アプリサーバ２００ａは、端末用精算終了画面データを生成し（ステップＳ１８４)、生成した端末用精算終了画面データを管理サーバ６００へ送信する（ステップＳ１８６)。

管理サーバ６００は、インターネット２０を介して、第１アプリサーバ２００ａから端末用精算終了画面データを受信し、受信した端末用精算終了画面データをユーザ端末１００へ送信する（ステップＳ１８８)。

ユーザ端末１００は、インターネット２０を介して管理サーバ６００から端末用精算終了画面データを受信し、受信した端末用精算終了画面データから精算終了画面１８１を生成し、モニタに表示する（ステップＳ１９１)。次に、利用者によるボタン操作を受け付け（ステップＳ１９２)、メニューボタン１８２の押下を受け付けると、ステップＳ１２１に戻りメニューの選択を受け付ける。

ログアウトボタン１８３の押下を受け付けると（ステップＳ１９２)、ユーザ端末１００は、ログアウトを示すログアウト通知を管理サーバ６００へ送信する（ステップＳ１９３)。

管理サーバ６００は、インターネット２０を介してユーザ端末１００からログアウト通知を受信し、受信したログアウト通知を第１アプリサーバ２００ａに送信する（ステップＳ１９４)。次に、ログアウト通知ト供に受信した端末ＩＤを含むログイン情報６３２を選択し、選択したログイン情報６３２をログインテーブル６３１から削除する（ステップＳ１９５)。また、図示していないが、第２アプリサーバ２００ｂ～第３アプリサーバ２００ｄへも同様にログアウト通知を送信する。

第１アプリサーバ２００ａは、インターネット２０を介して管理サー

バ６００からログアウト通知を受信する。ログアウト通知と供に受信した端末ＩＤを含むログイン情報を検索し、受信した端末ＩＤを含むログイン情報２３２が存在すれば、ログイン情報２３２をアプリログインテーブル２３１から削除する（ステップＳ１９６）。第２アプリサーバ２００ｂ～第４アプリサーバ２００ｄにおいても、同様にして自身の記憶しているアプリログインテーブル上に、受信した端末ＩＤを含むログイン情報が存在すれば、削除する。

（２）管理サーバ６００によるパスワード変更処理

管理サーバ６００によるパスワード変更処理について、図２７～図２９のフローチャートを用いて説明する。これは、図２０のステップＳ１２７の詳細である。

ユーザ端末１００は、アプリ番号「００５」を読み出し（ステップＳ３００）、読み出したアプリ番号「００５」とパスワード変更指示を管理サーバ６００へ送信する（ステップＳ３０１）。

管理サーバ６００は、インターネット２０を介して、アプリ番号「００５」とパスワード変更指示を受信する。パスワード変更指示を受信すると、端末用パスワード変更画面データを生成し（ステップＳ３０２）、生成した端末用パスワード変更画面データをユーザ端末１００へ送信する（ステップＳ３０３）。

ユーザ端末１００は、インターネット２０を介して、管理サーバ６００から端末用パスワード変更画面データを受信し、受信した端末用パスワード変更画面データからパスワード変更画面１９１を生成し、モニタに表示する（ステップＳ３０４）。次に、利用者による現パスワードと新パスワードの入力を受け付ける（ステップＳ３０６）。端末共通鍵を用いて、受け付けた現パスワードと新パスワードとを暗号化し、暗号化現パスワードと暗号化新パスワードとを生成する（ステップＳ３０７）。次に、生成した暗号化現パスワードと暗号化新パスワードとを、管理サーバ６００へ送信する（ステップＳ３０８）。

管理サーバ６００は、インターネット２０を介して、ユーザ端末１０

０から暗号化現パスワードと暗号化新パスワードとを受信する。暗号化現パスワードと暗号化新パスワードと供に受信した端末ＩＤを基に、ログインテーブル６３１内のログイン情報６３２を選択し、選択したログイン情報６３２の処理状況を「パスワード変更中」に書き換える（ステップＳ３０９）。

次に、端末共通鍵を用いて、受信した暗号化現パスワードと暗号化新パスワードを復号し、現パスワードと新パスワードとを生成する（ステップＳ３１１）。書き換えたログイン情報６３２に含まれるユーザＩＤを読み出し（ステップＳ３１２）、パスワードテーブル６２１内で、読み出したユーザＩＤと生成した現パスワードとを含むパスワード情報の有無を確認する（ステップＳ３１３）。

パスワードテーブル６２１内に、読み出したユーザＩＤと生成した現パスワードとを含むパスワード情報が、存在しなければ、認証が失敗であると判断し（ステップＳ３１６のＮＯ）、ステップＳ３０２へ戻り、再度、端末用パスワード変更画面データを送信する。

パスワードテーブル６２１内に、読み出したユーザＩＤと生成した現パスワードとを含むパスワード情報が、存在すれば、認証が成功であると判断する（ステップＳ３１６のＹＥＳ）。

次に、読み出しユーザＩＤと生成した現パスワードとを含むパスワード変更情報６５２をパスワード変更テーブル６５１から選択し（ステップＳ３１７）、選択したパスワード変更情報６５２に含まれる現パスワードと新パスワードとを生成した現パスワードと新パスワードとに書き換える（ステップＳ３１８）。

次に、第１アプリサーバ２００ａのパスワード変更処理を行い（ステップＳ３１９）、これが正常に終了すると、第２アプリサーバ２００ｂのパスワード変更処理を行い（ステップＳ３２１）、正常に終了しなければ図３２に示すパスワード復旧処理のステップＳ３６４へ処理を移す。第２アプリサーバ２００ｂのパスワード変更が正常に終了すると、第３アプリサーバ２００ｃのパスワード変更を行い（ステップＳ３２２）、正常

に終了しなければ図３２のステップＳ３６３へ処理を移す。第３アプリサーバ２００ｃのパスワード変更が正常に終了すると、第４アプリサーバ２００ｄのパスワード変更を行い（ステップＳ３２３）、正常に終了しなければ、図３２のステップＳ３６２へ処理を移す。第４アプリサーバ２００ｄのパスワード変更が正常に終了しなければ、図３２のステップＳ３６１へ処理を移す。

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄのパスワード変更が全て正常に終了すると、管理サーバ６００は、パスワードテーブル６２１から送信したユーザＩＤを含むパスワード情報を選択し、選択したパスワード情報に含まれるパスワードを新パスワードに書き換える。また、ログインテーブル６３１から送信したユーザＩＤを含むログイン情報６３２を選択し、選択したログイン情報６３２に含まれるパスワードを新パスワードに書き換える（ステップＳ３２６）。

次に、端末用変更完了画面データを生成し（ステップＳ３２７）、生成した端末用変更完了画面データをユーザ端末１００へ送信し（ステップＳ３２８）、ログイン情報６３２の処理状況を「通常」に書き換える（ステップＳ３２９）。

ユーザ端末１００は、インターネット２０を介して、管理サーバ６００から端末用変更完了画面データを受信し、受信した端末用変更完了画面データから変更完了画面３０１生成し、生成した変更完了画面３０１をモニタに表示する（ステップＳ３３１）。次に、利用者によるボタン操作を受け付け（ステップＳ３３２）、メニューボタン３０２の押下を受け付けると、ステップＳ１２１へ戻り、メニュー画面を表示する。

ログアウトボタン３０３の押下を受け付けると、管理サーバ６００へログアウト通知を送信し、処理を終了する（ステップＳ３３３）。

管理サーバ６００は、インターネット２０を介して、ユーザ端末１００からログアウト通知を受信する。受信したログアウト通知を第１アプリサーバ２００ａ～第４アプリサーバ２００ｄへ送信する（ステップＳ３３６）。次に、ログアウト通知と供に受信した端末ＩＤを基に、ログイ

ン情報６３２を選択し、選択したログイン情報６３２を消去する（ステップＳ３３４）。

アプリサーバ２００は、管理サーバ６００からログアウト通知を受信し、ログアウト通知と供に受信した端末ＩＤを含むログイン情報をアプリログインテーブル２３１内で検索し、受信した端末ＩＤを含むログイン情報を含むログイン情報が存在すれば、そのログイン情報を削除する（ステップＳ３３７）。

（３）アプリサーバ２００のパスワード変更処理

各アプリサーバ２００のパスワード変更処理について、図３０～３１に示すフローチャートを用いて説明する。なお、これは、図２８のステップＳ３１９、ステップＳ３２１、ステップＳ３２２及びステップＳ３２３の詳細である。

管理サーバ６００は、アプリサーバ２００と相互認証を行いサーバ共通鍵を生成する（ステップＳ３４１）。ステップＳ３１８において書き換えたパスワード変更情報６５２から、ユーザＩＤと現パスワードと新パスワード抽出し、サーバ共通鍵を用いて、抽出した現パスワードと新パスワードとを暗号化し、暗号化現パスワードと暗号化新パスワードとを生成する（ステップＳ３４２）。抽出したユーザＩＤと生成した暗号化現パスワードと暗号化新パスワードとをアプリサーバ２００へ送信し、パスワード変更を指示する（ステップＳ３４３）。次に、パスワード変更指示を送信してからの経過時間を計測するｔｉｍｅカウンタを０に設定し、経過時間の計測を開始する（ステップＳ３４４）。

アプリサーバ２００は、インターネット２０を介して管理サーバ６００から、ユーザＩＤと暗号化現パスワードと暗号化新パスワードとを受信し、暗号化を指示される。サーバ共通鍵を用いて、受信した暗号化現パスワードと暗号化新パスワードとを復号し、現パスワードと新パスワードとを生成する（ステップＳ３４５）。

パスワードテーブル２２１内で受信したユーザＩＤを含むパスワード情報２２３を選択し、選択したパスワード情報２２３に含まれるパスワ

ードを新パスワードに書き換える（ステップＳ３４６）。パスワードの書き換えが成功であると判断すると（ステップＳ３４７のＹＥＳ）、終了信号「１」を生成する（ステップＳ３４９）。パスワードの書き換えが失敗であると判断すると（ステップＳ３４７のＮＯ）、終了信号「０」を生成する（ステップＳ３４８）。

次に、生成した終了信号を、インターネット２０を介して、管理サーバ６００へ送信する（ステップＳ３５１）。

管理サーバ６００は、アプリサーバ２００から終了信号を受信すると（ステップＳ３５５のＹＥＳ）、受信した終了信号を判別し（ステップＳ３５６）、終了信号「１」であると判断すると、アプリサーバ２００のパスワード変更を終了する。

終了信号「０」であると判断すると（ステップＳ３５６の「０」）、パスワード復旧処理へ移行する（ステップＳ３５９）。

アプリサーバ２００から、終了信号を受信していなければ（ステップＳ３５５のＮＯ）、ｔｉｍｅカウンタの値と最大待ち時間とを比較し（ステップＳ３５８）、ｔｉｍｅカウンタが最大待ち時間を超えていないと判断すると（ステップＳ３５８のＮＯ）、ステップＳ３５５へ戻り、アプリサーバ２００から終了信号を受信するかｔｉｍｅカウンタが最大待ち時間を超えるまで、ステップＳ３５５～ステップＳ３５８の処理を繰り返す。

ｔｉｍｅカウンタが最大待ち時間を超えていると判断すると（ステップＳ３５８のＹＥＳ）、アプリサーバ２００のパスワード変更が失敗あると判断し、パスワード復旧処理を行う（ステップＳ３５９）。

（４）管理サーバ６００によるパスワード復旧処理

管理サーバ６００によるパスワード復旧の処理について、図３２のフローチャートを用いて説明する。これは、図３１のステップＳ３５９の詳細である。

ただし、図２８のステップＳ３１９の処理中であればステップＳ３６４からパスワード復旧処理を開始する。ステップＳ３２１の処理中であ

れば、ステップＳ３６３からパスワード復旧処理を開始し、ステップＳ３２２の処理中であれば、ステップＳ３６２から、パスワード復旧の処理を開始する。図２８のステップＳ３２３の処理中であれば、ステップＳ３６１からパスワード復旧の処理を開始する。

管理サーバ６００は、第３アプリサーバ２００ｃのパスワード復旧を行い（ステップＳ３６１）、これが正常に終了すれば、第２アプリサーバ２００ｂのパスワード復旧を行う（ステップＳ３６２）。ステップＳ３６２が正常に終了すれば、第１アプリサーバ２００ａのパスワード復旧を行う（ステップＳ３６３）。

ステップＳ３６４が正常に終了すると、管理サーバ６００は、変更失敗画面とログイン情報６３２とを基に、端末用変更失敗画面データを生成し（ステップＳ３６４）、生成した端末用変更失敗画面データをユーザ端末１００へ送信する（ステップＳ３６６）。

ユーザ端末１００は、インターネット２０を介して、管理サーバ６００から端末用変更失敗画面データを受信し、受信した端末用変更失敗画面データから変更失敗画面３１１を生成し、生成した変更失敗画面３１１をモニタに表示する（ステップＳ３６７）。次に、利用者のボタン操作を受け付け（ステップＳ３６８）、メニューボタン３１２の選択を受け付けると、ステップＳ１２１へ処理を移す。

ログアウトボタン３１３の選択を受け付けると、管理サーバ６００へログアウト通知を送信する（ステップＳ３７１）。

管理サーバ６００は、インターネット２０を介してユーザ端末１００からログアウト通知を受信し、ログアウト通知と供に受信した端末ＩＤを基に、ログイン情報６３２を選択し、選択したログイン情報６３２を削除する（ステップＳ３７２）。

また、具体的には図示していないが、受信したログアウト通知をアプリサーバ２００へ送信する。アプリサーバ２００は、インターネット２０を介して管理サーバ６００からログアウト通知を受信し、ログアウト通知と供に受信した端末ＩＤを含むログイン情報をアプリログインテー

ブル２３１内で検索し、端末ＩＤを含むログイン情報が存在すれば、該当するログイン情報を削除する。

（５）アプリサーバ２００のパスワード復旧処理

アプリサーバ２００のパスワード復旧処理について、図３３に示すフローチャートを用いて説明する。これは、図３２のステップＳ３６１、ステップＳ３６２、ステップＳ３６３の詳細である。

管理サーバ６００は、パスワード復旧指示の送信回数をカウントする回数カウンタを０に設定する（ステップＳ３８０）。次に、パスワード変更情報６５２に含まれる、ユーザＩＤと現パスワードと新パスワードと読み出し、サーバ共通鍵を用いて、読み出した現パスワードと新パスワードとを暗号化し、暗号化現パスワードと暗号化新パスワードとを生成する（ステップＳ３８１）。次に、読み出しユーザＩＤと生成した暗号化現パスワードと暗号化新パスワードとをアプリサーバ２００へ送信しパスワード復旧を指示する（ステップＳ３８２）。次に、パスワード復旧指示を送信してからの経過時間を計測するｔｉｍｅカウンタを０に設定し、経過時間の計測を開始する（ステップＳ３８３）

アプリサーバ２００は、インターネット２０を介して管理サーバ６００から、ユーザＩＤと暗号化現パスワードと暗号化新パスワードとを受信し、パスワード復旧の指示を受け取る。サーバ共通鍵を用いて受信した暗号化現パスワードと暗号化しパスワードとを復号し、現パスワードと新パスワードとを生成する（ステップＳ３８４）。次に、パスワードテーブル２２１上で受信したユーザＩＤと生成した新パスワードとを含むパスワード情報を選択し、選択したパスワード情報のパスワードを現パスワードに書き換える（ステップＳ３８５）。

パスワードの書き換えが成功であれば（ステップＳ３８６のＹＥＳ）、終了通知「１」を生成する（ステップＳ３８７）。パスワードの書き換えが失敗であれば（ステップＳ３８６のＮＯ）、終了信号「０」を生成する（ステップＳ３８８）。　次に、生成した終了信号を管理サーバ６００へ送信する（ステップＳ３８９）。

管理サーバ６００は、インターネット２０を介して、アプリサーバ２００から終了信号を受信すると（ステップＳ３９１のＹＥＳ）、受信した終了信号を判別し（ステップＳ３９２）、終了信号「１」であると判断すると、これをもって、アプリサーバ２００のパスワード復旧を正常に終了する。

終了信号「０」であると判断すると（ステップＳ３９２）、ステップＳ３９６へ処理を移す。

アプリサーバ２００から、終了信号を受信していなければ（ステップＳ３９１のＮＯ）、ｔｉｍｅカウンタの値と最大待ち時間とを比較し（ステップＳ３９４）、ｔｉｍｅカウンタが最大待ち時間を超えていないと判断すると（ステップＳ３９４のＮＯ）、ステップＳ３９１へ戻り、アプリサーバ２００から終了信号を受信するかｔｉｍｅカウンタが最大待ち時間を超えるまで、ステップＳ３９１～ステップＳ３９４の処理を繰り返す。

ｔｉｍｅカウンタが最大待ち時間を超えていると判断すると（ステップＳ３９４のＹＥＳ）、回数カウンタに１加算し（ステップＳ３９６）、次に回数カウンタの値と制限回数を比較し（ステップＳ３９７）、制限回数を超えていなければ（ステップＳ３９７のＮＯ）、ステップＳ３８２へ処理を移す。

制限回数を超えていると判断すると（ステップＳ３９７のＹＥＳ）、パスワード復旧の失敗であると判断し、端末用強制終了画面データを生成し（ステップＳ３９８）、生成した端末用強制終了画面データをユーザ端末１００へ送信する（ステップＳ３９９）。

次に、エラー画面３３１を生成し（ステップＳ４０２）、生成したエラー画面を表示部６１３に表示する（ステップＳ４０３）。

ユーザ端末１００は、インターネット２０を介して、管理サーバ６００から端末用強制終了画面データを受信する。受信した端末用強制終了画面データから強制終了画面３２１を生成し、モニタに表示し（ステップＳ４０１）、処理を終了する。

（６）相互認証処理

機器間での相互認証の動作について図３５～図３６を用いて説明する。

なお、この相互認証の方法は一例であり、他の認証方法、鍵共有方法を用いてもよい。また、相互認証は、ユーザ端末１００と管理サーバ６００の間又は管理サーバ６００とアプリサーバ２００の間で行うため、ここでは双方の機器を、機器Ａ及び機器Ｂとして説明する。上記の説明では、ユーザ端末１００と管理サーバ６００の間の相互認証により生成される共通鍵を端末共通鍵、管理サーバ６００とアプリサーバ２００の間の相互認証により生成される共通鍵をサーバ共通鍵と呼称している。

ここで、Ｇｅｎ（）を鍵生成関数とし、Ｙをシステム固有のパラメータとする。鍵生成関数Ｇｅｎ（）は、Ｇｅｎ（ｘ，Ｇｅｎ（ｚ，Ｙ））＝Ｇｅｎ（ｚ，Ｇｅｎ（ｘ，Ｙ））の関係を満たすものとする。鍵生成関数は任意の公知技術で実施可能なため、詳細についてここでは説明しない。

機器Ａは、公開鍵証明書Ｃｅｒｔ＿Ａを読み出し（ステップＳ２０１）、読み出した公開鍵証明書Ｃｅｒｔ＿Ａを機器Ｂへ送信する（ステップＳ２０２）。

公開鍵証明書Ｃｅｒｔ＿Ａを受信した機器Ｂは、認証局の公開鍵ＰＫ＿ＣＡを用いて、公開鍵証明書Ｃｅｒｔ＿Ａに含んで受信した認証局の署名データＳｉｇ＿ＣＡに署名検証アルゴリズムＶを施して署名検証する（ステップＳ２０３）。ここで、署名検証アルゴリズムＶは、署名生成アルゴリズムＳにより生成された署名データを検証するアルゴリズムである。署名検証の結果が失敗であれば（ステップＳ２０４のＮＯ）処理を終了する。

署名検証の結果が成功であれば（ステップＳ２０４のＹＥＳ）、機器Ｂは、ＣＲＬを読み出し（ステップＳ２０５）、公開鍵証明書Ｃｅｒｔ＿Ａに含んで受信したＩＤ番号ＩＤ＿Ａが読み出したＣＲＬに登録されているか否かを判断する（ステップＳ２０６）。登録されていると判断すると（ステップＳ２０６のＹＥＳ）、処理を終了する。

登録されていないと判断すると（ステップＳ２０６のＮＯ）、機器Ｂは、

公開鍵証明書Ｃｅｒｔ＿Ｂを読み出し（ステップＳ２０７）、読み出した公開鍵証明書Ｃｅｒｔ＿Ｂを機器Ａに送信する。

公開鍵証明書Ｃｅｒｔ＿Ｂを受信した機器Ａは、認証局の公開鍵ＰＫ＿ＣＡを用いて、公開鍵証明書Ｃｅｒｔ＿Ｂに含んで受信した認証局の署名データＳｉｇ＿ＣＡに署名検証アルゴリズムＶを施して署名検証する（ステップＳ２０９）。署名検証の結果が失敗であれば（ステップＳ２１０のＮＯ）処理を終了する。

署名検証の結果が成功であれば（ステップＳ２１０のＹＥＳ）、機器Ａは、ＣＲＬを読み出し（ステップＳ２１１）、公開鍵証明書Ｃｅｒｔ＿Ｂに含んで受信したＩＤ番号ＩＤ＿Ｂが読み出したＣＲＬに登録されているか否かを判断する（ステップＳ２１２）。登録されていると判断すると（ステップＳ２１２のＹＥＳ）、処理を終了する。登録されていないと判断すると（ステップＳ２１２のＮＯ）、処理を継続する。

機器Ｂは、乱数Ｃｈａ＿Ｂを生成し（ステップＳ２１３）、生成した乱数Ｃｈａ＿Ｂを機器Ａに送信する（ステップＳ２１４）。

機器Ａは、乱数Ｃｈａ＿Ｂを受信し、機器Ａの秘密鍵ＳＫ＿Ａを用いて、受信した乱数Ｃｈａ＿Ｂに署名生成アルゴリズムＳを施して署名データＳｉｇ＿Ａを生成し（ステップＳ２１５）、生成した署名データＳｉｇ＿Ａを機器Ｂへ送信する（ステップＳ２１６）。

機器Ｂは、署名データＳｉｇ＿Ａを受信すると、公開鍵証明書Ｃｅｒｔ＿Ａに含んで受信した機器Ａの公開鍵ＰＫ＿Ａを用いて、受信した署名データＳｉｇ＿Ａに、署名検証アルゴリズムＶを施して署名検証する（ステップＳ２１７）。署名検証の結果が失敗であると判断すると（ステップＳ２１８のＮＯ）処理を終了する。署名検証の結果が成功であると判断すると（ステップＳ２１８のＹＥＳ）、処理を続ける。

機器Ａは、乱数Ｃｈａ＿Ａを生成し（ステップＳ２１９）、生成した乱数Ｃｈａ＿Ａを機器Ａに送信する（ステップＳ２２０）。

機器Ｂは、乱数Ｃｈａ＿Ａを受信し、機器Ｂの秘密鍵ＳＫ＿Ｂを用いて、受信した乱数Ｃｈａ＿Ａに署名生成アルゴリズムＳを施して署名デ

ータＳｉｇ＿Ｂを生成し（ステップＳ２２１）、生成した署名データＳｉｇ＿Ｂを機器Ａへ送信する（ステップＳ２２２）。

機器Ａは、署名データＳｉｇ＿Ｂを受信すると、公開鍵証明書Ｃｅｒｔ＿Ｂに含んで受信した機器Ｂの公開鍵ＰＫ＿Ｂを用いて、受信した署名データＳｉｇ＿Ｂに、署名検証アルゴリズムＶを施して署名検証する（ステップＳ２２３）。署名検証の結果が失敗であると判断すると（ステップＳ２２４のＮＯ）処理を終了する。署名検証の結果が成功であると判断すると（ステップＳ２２４のＹＥＳ）、次に、乱数「ａ」を生成し（ステップＳ２２５）、生成した乱数「ａ」を用いてＫｅｙ＿Ａ＝Ｇｅｎ（ａ，Ｙ）を生成し（ステップＳ２２６）、生成したＫｅｙ＿Ａを機器Ｂへ送信する（ステップＳ２２７）。

機器Ｂは、Ｋｅｙ＿Ａを受信すると、乱数「ｂ」を生成し（ステップＳ２２８）、生成した乱数「ｂ」を用いてＫｅｙ＿Ｂ＝Ｇｅｎ（ｂ，Ｙ）を生成し（ステップＳ８２９）、生成したＫｅｙ＿Ｂを機器Ａへ送信する（ステップＳ２３０）。

また、生成した乱数「ｂ」と受信したＫｅｙ＿Ａとを用いて、Ｋｅｙ＿ＡＢ＝Ｇｅｎ（ｂ，Ｋｅｙ＿Ａ）＝Ｇｅｎ（ｂ，Ｇｅｎ（ａ，Ｙ））を生成し、これを共通鍵とする（ステップＳ２３１）。

機器Ａは、Ｋｅｙ＿Ｂを受信し、生成した乱数「ａ」と受信したＫｅｙ＿ＢとからＫｅｙ＿ＡＢ＝Ｇｅｎ（ａ，Ｋｅｙ＿Ｂ）＝Ｇｅｎ（ａ，Ｇｅｎ（ｂ，Ｙ））を生成し、これを共通鍵とする（ステップＳ２３２）。

（７）パスワード変更の実行例

以下に、パスワード変更の１実行例を図３７を用いて説明する。ここでは、ユーザＩＤ「ｍａｅｄａ」の利用者の現パスワード「ｏｚｙ１２」を新パスワード「ｎｗｙ５６」に変更する。ユーザ端末１００と管理サーバ６００間の通信及び管理サーバ６００とアプリサーバ２００間の通信において、現パスワード及び新パスワードは、端末共通鍵又はサーバ共通鍵を用いた秘密通信により安全に送受信されるが、以下の説明において、簡略化のため、暗号化及び復号の処理についての説明を省略する。

変更前の各アプリサーバ２００は、図３７（ａ）に示すようにユーザＩＤ「ｍａｅｄａ」に対応するパスワード「ｏｚｙ１２」を記憶している。

ユーザ端末１００からのパスワード変更指示により、管理サーバ６００は、ユーザ端末１００へ端末用パスワード変更画面データを送信する。

ユーザ端末１００は、端末用パスワード変更画面データを受信し、受信した端末用パスワード変更画面データからパスワード変更画面１９１生成し表示する。利用者による現パスワード「ｏｚｙ１２」と新パスワード「ｎｗｙ５６」の入力を受け付け、受け付けた現パスワード「ｏｚｙ１２」と新パスワード「ｎｗｙ５６」を、管理サーバ６００へ送信する。

管理サーバ６００は、ユーザ端末１００から現パスワード「ｏｚｙ１２」と新パスワード「ｎｗｙ５６」を受信する。次に、第１アプリサーバ２００ａへ受信した現パスワード「ｏｚｙ１２」と新パスワード「ｎｗｙ５６」とを送信しパスワードの変更を指示する。

第１アプリサーバ２００ａは、自身の記憶している現パスワード「ｏｚｙ１２」を新パスワード「ｎｗｙ５６」に書き換え、終了信号「１」を送信する。

第１アプリサーバ２００ａから、正常にパスワード変更が終了したことを示す終了信号「１」を受信すると、管理サーバ６００は、第２アプリサーバ２００ｂにも同様に現パスワード「ｏｚｙ１２」と新パスワード「ｎｗｙ５６」とを送信しパスワードの変更を指示し、終了信号「１」を受信する。このとき、第１アプリサーバ２００ａ及び第２アプリサーバ２００ｂは、図３７ｂに示すように、新パスワード「ｎｗｙ５６」を記憶しており、第３アプリサーバ２００ｃと第４アプリサーバ２００ｄは、現パスワード「ｏｚｙ１２」を記憶している。

管理サーバ６００は、次に、第３アプリサーバ２００ｃに現パスワード「ｏｚｙ１２」と新パスワード「ｎｗｙ５６」とを送信しパスワードの変更を指示する。

ここで、第３アプリサーバ２００ｃは、パスワードの変更を失敗し、終了信号「０」を管理サーバ６００へ送信する。

第３アプリサーバ２００ｃから、パスワードの変更が失敗であることを示す終了信号「０」を受け取ると、管理サーバ６００は、第２アプリサーバ２００ｂへ現パスワード「ｏｚｙ１２」と新パスワード「ｎｗｙ５６」とを送信しパスワードの復旧を指示する。次に、管理サーバ６００は、第２アプリサーバ２００ｂから、パスワードの復旧が成功したことを示す終了信号「１」を受け取る。次に、第１アプリサーバ２００ａにも同様に、パスワード復旧を指示し、第１アプリサーバ２００ａから終了信号「１」を受け取る。これをもって、パスワードの復旧の完了とする。このとき、各アプリサーバは、図３７（ｃ）の示すように、現パスワード「ｏｚｙ１２」を記憶している。

図３７（ｄ）は、第３アプリサーバ２００ｃ及び第４アプリサーバ２００ｄのパスワード変更が成功した場合に各アプリサーバが記憶しているパスワードを示している。

１．６まとめ

上記に、説明したように、本実施の形態によると、管理サーバ６００は、ユーザ端末１００から、パスワードの変更指示を受け取る。管理サーバ６００は、端末秘密鍵を用いた秘密通信により、ユーザ端末１００から安全に現パスワードと新パスワードとを受信する。

次に、サーバ共通鍵を用いた秘密通信により、安全に現パスワードと新パスワードとを第１アプリサーバ２００ａへ送信しパスワードの変更を指示する。第１アプリサーバ２００ａのパスワード変更が成功であれば、同様にして、第２アプリサーバ２００ａ～第４アプリサーバ２００ｄの順にパスワードの変更を指示する。

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄのいずれかでパスワードの変更が失敗すると、既にパスワード変更が終了したアプリサーバに対して、現パスワードと新パスワードとを送信しパスワードの復旧を指示する。

このようにして、複数のアプリサーバのうちいずれかがパスワードの変更に失敗した場合でも、複数のアプリサーバのパスワードを統一することができる。

２．実施の形態２

以下に実施の形態２のパスワード変更システムについて、説明する。

パスワード変更システムは図３８に示すように、ユーザ端末１００、内部ユーザ端末１５０、１６０・・・、第１アプリサーバ２００ａ、第２アプリサーバ２００ｂ、第３アプリサーバ２００ｃ、第４アプリサーバ２００ｄ、管理サーバ６００ｂ及びルータ８００から構成される。

第２アプリサーバ２００ｂ～第４アプリサーバ２００ｄ及び管理サーバ６００ｂは、バス３１に接続されており、バス型ＬＡＮを形成している。内部ユーザ端末１５０、１６０・・・及び管理サーバ６００ｂは、バス３２に接続されており、バス型ＬＡＮを形成している。バス３１及び３２は、具体的には、両端に終端装置を備えた同軸ケーブルである。

管理サーバ６００ｂは、さらに、ファイアウォール機能を備えるルータ８００を介してインターネットと接続されている。

管理サーバ６００ｂ、第２アプリサーバ２００ｂ～第４アプリサーバ２００ｄ及び内部ユーザ端末１５０、１６０・・・は、一例として、同一の建物内のＬＡＮを構成している。

ユーザ端末１００と第１アプリサーバ２００は、インターネット２０に接続されている。

実施の形態１と同様に、管理サーバ６００ｂ及び第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、あらかじめ正当な利用者のユーザＩＤとパスワードを対応付けて記憶している。

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、それぞれ、出張費精算、休暇申請、会議室予約及び従業員購入のサービスを提供する。

利用者は、ユーザ端末１００を用いて、インターネット２０及び管理サーバ６００ｂを介して、これらのサービスを利用する。また、内部ユ

ーザ端末１５０、１６０・・・を用いて、バス３１及び３２を介して、これらサービスを利用することもできる。

このとき、ユーザ端末１００又内部ユーザ端末１５０、１６０・・・は、管理サーバ６００ｂに利用者のユーザＩＤとパスワードを送信する。

管理サーバ６００ｂ及び第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、ユーザ端末１００又内部ユーザ端末１５０、１６０・・・から送信されたユーザＩＤとパスワードを検証し、ユーザ端末１００又内部ユーザ端末１５０、１６０・・・の利用者が正当な利用者であることを認証し、各アプリサーバは、それぞれが備えるサービスを提供する。

また、管理サーバ６００ｂは、ユーザ端末１００又内部ユーザ端末１５０、１６０・・・からパスワード変更の指示と現在のパスワードと新しいパスワードとを受信する。管理サーバ６００ｂは、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄへ、受け取った新しいパスワードを順次送信し、パスワードの変更を指示する。

ここで、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄの何れかで、パスワードの変更が正常に行われなかった場合、管理サーバ６００ｂは、既にパスワード変更が終了しているアプリサーバに現在のパスワードを送信し、現在のパスワードへパスワードを変更し直すように指示する。

ユーザ端末１００、内部ユーザ端末１５０、１６０・・・の具体的な構成及び動作は、実施の形態１のユーザ端末１００と同一であるので説明を省略する。

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄの具体的な構成及び動作は、実施の形態１の第１アプリサーバ２００ａ～第４アプリサーバ２００ｄと同一であるので説明を省略する。

管理サーバ６００ｂは、図３９に示すように、送受信部６０１ｂ、認証部６０３、パスワード変更部６０６、制御部６０７、暗号処理部６０８、パスワード復旧部６１４、変更判定部６０９、変更結果通知部６１５、情報記憶部６１０、入力部６１２及び表示部６１３から構成される。

送受信部６０１ｂは、バス３１、３２及びバス３５と接続されている。送受信部６０１ｂは、バス３１を介して、第２アプリサーバ２００ｂ～第４アプリサーバ２００ｄと管理サーバ６００ｂ内の各部との間で情報の送受信を行い、バス３２を介して、内部ユーザ端末１５０、１６０・・・と管理サーバ６００ｂ内の各部との間で情報の送受信を行う。また、バス３５、ルータ２０及びインターネット２０を介してユーザ端末１００及び第１アプリサーバ２００ａと管理サーバ６００ｂ内の各部との間で、情報の送受信を行う。

この際、第２アプリサーバ２００ｂ～第４アプリサーバ２００ｄとの情報の送受信においては、送受信部６０１ｂは、バス３１を選択し、内部ユーザ端末１５０、１６０・・・との情報の送受信においては、バス３２を選択する。また、ユーザ端末１００及び第１アプリサーバ２００ａとの情報の送受信においては、バス３５を選択する。

送受信部６０１ｂのその他の具体的な動作は、実施の形態１の送受信部６０１と同様である。

また、認証部６０３、パスワード変更部６０６、制御部６０７、暗号処理部６０８、パスワード復旧部６１４、変更判定部６０９、変更結果通知部６１５、入力部６１２、表示部６１３の具体的な動作及び情報記憶部６１０の構成は、図１３を用いで説明した実施の形態１と同様である。

ルータ８００は、ファイヤウォール機能を備えており、インターネット２０に接続された外部機器から、ＬＡＮ内の各機器宛に送信された各種の情報の通過又は遮断を行う。具体的には、インターネットを介して受信したパケットに含まれる、送信元及び送信先のＩＰアドレスやポート番号が、あらかじめ設定された条件を満たしているか否かを判断し、条件を満たしていれば通過させ、満たしていなければ受信したパケットを削除する。このような方法は、一般的にパケットフィルタリングといわれる。また、このファイヤウォール機能は一例であり、他の方法を用いてもよい。

以上に説明したように、本実施の形態では、ルータ８００のファイヤウォール機能により、インターネット２０に接続された不正な外部機器による攻撃から管理サーバ６００ｂ及びＬＡＮに接続されている各機器を防御することができる。

３．実施の形態３

以下に実施の形態３のパスワード変更システムについて、説明する。

パスワード変更システムは、図４０に示すように、ユーザ端末１７０、１８０・・・、第１アプリサーバ２００ａ～第４アプリサーバ２００及び管理サーバ６００ｃから構成される。

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄ及び、管理サーバ６００ｃはバス３３に接続されておりバス型ＬＡＮを形成している。ユーザ端末１７０、１８０・・・と管理サーバ６００ｃは、バス３４に接続されており、バス型ＬＡＮを形成している。バス３３及び３４は、具体的には、両端に終端装置を備える同軸ケーブルである。

管理サーバ６００ｃ、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄ及びユーザ端末１７０、１８０・・・は、一例として、同一の建物内のＬＡＮを構成している。

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、それぞれ、出張費精算、休暇申請、会議室予約及び従業員購入のサービスを提供する。

利用者は、ユーザ端末１７０、１８０・・・のうち何れかを使用し、管理サーバ６００ｃを介して第１アプリサーバ２００～第４アプリサーバ２００ｄの提供するサービスを利用する。

このとき、利用者の使用するユーザ端末１７０は、管理サーバ６００ｃに利用者のユーザＩＤとパスワードを送信する。

管理サーバ６００ｃ及び第１アプリサーバ２００ａ～第４アプリサーバ２００ｄは、ユーザＩＤとパスワードを検証し、ユーザ端末１００の利用者が正当な利用者であることを認証し、各アプリサーバ２００は、ぞれぞれが備えるサービスを提供する。

また、管理サーバ６００ｃは、ユーザ端末１７０からパスワード変更の指示を受信し、ユーザ端末１００から、現在のパスワードと新しいパスワードとを受信する。管理サーバ６００ｃは、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄへ、受け取った新しいパスワードを順次送信し、パスワードの変更を指示する。

ここで、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄの何れかで、パスワードの変更が正常に行われなかった場合、管理サーバ６００ｃは、既にパスワード変更が終了しているアプリサーバに現在のパスワードを送信し、現在のパスワードへパスワードを変更し直すように指示する。

第１アプリサーバ２００ａ～第４アプリサーバ２００ｄの具体的な構成及び動作はそれぞれ実施の形態１の第１アプリサーバ２００ａ～第４アプリサーバ２００ｄと同様であるので説明を省略する。

ユーザ端末１７０、１８０・・・の具体的な構成及び動作は実施の形態１のユーザ端末１００と同様であるので説明を省略する。

管理サーバ６００ｃは、図４１に示すように、送受信部６０１ｃ、認証部６０３、パスワード変更部６０６、制御部６０７、暗号処理部６０８、パスワード復旧部６１４、変更判定部６０９、変更結果通知部６１５、情報記憶部６１０、入力部６１２及び表示部６１３から構成される。

送受信部６０１ｃは、バス３３を介して、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄと管理サーバ６００ｃ内の各部との間で情報の送受信を行う。バス３４を介してユーザ端末１７０、１８０・・・と管理サーバ６００ｃ内部の各部との間で情報の送受信を行う。

この際、第１アプリサーバ２００ａ～第４アプリサーバ２００ｄとの情報の送受信において、送受信部６０１ｃは、バス３３を選択し、ユーザ端末１７０、１８０・・・との情報の送受信において、バス３４を選択する。

送受信部６０１ｃの具体的な動作は、実施の形態１の送受信部６０１と同様である。

認証部６０３、パスワード変更部６０６、制御部６０７、暗号処理部６０８、パスワード復旧部６１４、変更判定部６０９、変更結果通知部６１５、入力部６１２及び表示部６１３の具体的な動作、情報記憶部６１０の構成は実施の形態１の管理サーバ６００と同様であるので説明を省略する。

本実施の形態では、アプリサーバ２００は管理サーバ６００ｃを介してユーザ端末１７０、１８０と接続されている。利用者が、ユーザ端末１７０及び１８０を使用して、アプリサーバ２００の提供するサービスを利用する際に送受信される各種の情報は必ず管理サーバ６００ｃを通過するため、管理サーバ６００ｃは、悪意のある利用者による不正なサービスの利用を発見しやすくなる。

また、本実施の形態のように、閉じたＬＡＮの場合又はファイヤウォール等により保護されたＬＡＮ内のみで上述したサービス提供及びパスワード変更に係る通信を行う場合、認証部６０３による相互認証を省略することもできる。これにより、上述したサービス提供の処理及びパスワード変更の処理をより迅速に行うことができる。

４．その他の変形例

（１）管理サーバによるパスワード変更開始

上記の実施の形態１～３において、ユーザ端末又は内部ユーザ端末からパスワード変更の要求を受信することにより、パスワード変更の処理を開始しているが、管理サーバ６００から利用者にパスワードの変更を促してもよい。

具体的には、管理サーバ６００は、あらかじめパスワードの最長使用期間を記憶している。また、利用者が主に使うユーザ端末のＩＰアドレスを、利用者のユーザＩＤと対応付けて記憶している。パスワードテーブル６２１に代わって、パスワードテーブル６２１ｂを記憶している。

パスワードテーブル６２１ｂは、図４２に示すように、複数のパスワード情報６２２ｂ、６２３ｂ、６２４ｂ・・・から構成される。各パスワード情報は、ユーザＩＤ、氏名、パスワード及び更新日を含む。ユー

ザＩＤ、氏名及びパスワードは、上記の実施の形態のパスワードテーブル６２１に含まれるユーザＩＤ、氏名及びパスワードと同様であるので説明を省略する。更新日は、パスワード情報に含まれるパスワードが変更された最近の日付を示しており、例えばパスワード情報６２２ｂに含まれるパスワードは、２００年５月１０日に「ｏｚｙ１２」に変更されたことを示す。

管理サーバ６００は、定期的に各パスワード情報に含まれる変更日をチェックし、最長使用期間を超えてパスワードの変更を行っていない利用者に対し、あらかじめ記憶しているユーザ端末へ、パスワードが最長使用期間を過ぎていることを通知するメッセージを送信し、パスワードの変更を促す。

（２）強制パスワード変更

また上記の（１）において、最長使用期間を超えてパスワードを変更していない利用者が、各種サービスを利用しようとするときに、強制的にパスワード変更を促してもよい。

具体的には、上記の実施の形態１～３において、管理サーバ６００は、ユーザ端末からユーザＩＤと暗号化パスワードを受信すると、先ず、パスワードテーブル６２１ｂ内で受信したユーザＩＤを含むパスワード情報６２２ｂを選択する。選択したパスワード情報６２２ｂに含まれる変更日を読み出す。読み出した更新日に、最長使用期間（例えば３０日）を加算した変更期限「２０００．６．９」を算出し、算出した変更期限「２０００．６．９」と現在の日付とを比較する。現在の日付が変更期限「２０００．６．９」を越えていると判断すると、管理サーバ６００は、ユーザ端末に端末用パスワード変更画面データを送信し、パスワードの変更を行わなければ、サービスの利用ができないようにしてもよい。

（３）アプリサーバ２００への問合せ

また、実施の形態１～３では、管理サーバ６００は各アプリサーバ２００にユーザＩＤと暗号化現パスワードと暗号化新パスワードとパスワード変更指示とを同時に送信しているが、各アプリサーバ２００にあら

かじめパスワードの変更が可能か否かを問合せ、全てのアプリサーバ２００が、パスワード変更可能である場合にのみ、パスワード変更を指示するとしてもよい。

具体的には、管理サーバ６００は、まず、第１アプリサーバ２００ａにユーザＩＤと暗号化現パスワードと暗号化新パスワードとを送信し、パスワード変更が可能か否かを問い合わせる。

第１アプリサーバ２００ａは、管理サーバ６００からユーザＩＤと暗号化現パスワードと暗号化新パスワードを受信し、パスワード変更が可能か否かの問合せを受け付けると、パスワード変更が可能か否かを示す応答信号を生成する。パスワードの変更が書き換え可能であれば、応答信号「１」、ハードディスク障害などによりパスワードの書き換えが不可能であれば応答信号「０」を生成し、生成した応答信号を管理サーバ６００へ送信する。

管理サーバは、第１アプリサーバ２００ａから応答信号を受信し、受信した応答信号が「１」であれば、第２アプリサーバ２００ｂにも同様にしてユーザＩＤと暗号化現パスワードと暗号化新パスワードとを送信し、パスワード変更が可能か否かを問い合わせ、応答信号「１」を受信すると、次のアプリサーバ２００へ、同様の問合せを行う。

全てのアプリサーバ２００から、応答信号「１」を受信すると、管理サーバ６００は、全てのアプリサーバ２００へ、パスワード変更を指示する。

各アプリサーバ２００は管理サーバ６００からパスワード変更の指示を受信し、前もって受信している暗号化現パスワードと暗号化新パスワードとを復号して、現パスワードと新パスワードとを生成し、受信したユーザＩＤと生成した現パスワードとを含むパスワード情報を選択し、選択したパスワード情報に含まれるパスワードを生成した新パスワードに書き換える。

次に、管理サーバ６００は、ユーザ端末に端末用変更完了画面データを送信し、パスワードの変更が正常に終了したことを通知する。

パスワード変更が可能か否かの問合せの途中に、何れかのアプリサーバ２００から応答信号「０」を受信すると、該当するアプリサーバ２００のパスワード変更は不可能であると判断し、既にパスワード変更の問合せを行ったアプリサーバ２００全てに、パスワード変更の中止を知らせる。

次に、ユーザ端末に端末用変更失敗画面データを送信し、パスワード変更が失敗したことを通知する。

（４）タイムアウトによる判断

また上記の（３）において、各アプリサーバ２００にパスワード変更が可能か否かを問い合わせる際に、問合せを送信してからの時間を計測し、あらかじめ設定しておいた最大待ち時間を超えても応答信号を受信しないとき、該当するアプリサーバ２００のパスワード変更は不可能であると判断するとしてもよい。

（５）専用線による接続

実施の形態３において、パスワード変更システムは、パスワード変更用の専用線を備えるとしてもよい。

具体的には、管理サーバ６００と各アプリサーバ２００とは専用線で直接接続されている。通常のサービスの提供には、上記の実施の形態３において説明したように、バス３３及び３４を介して、情報の送受信を行う。

（６）アプリサーバ２００の処理状況

上記の実施の形態１～３において、管理サーバ６００は、各アプリサーバ２００の処理状況を記憶しており、これに応じてパスワードの変更の実施を中止するとしてもよい。

具体的には、管理サーバ６００は、ルーティングテーブル６４１に代わって、ルーティングテーブル６４１ｂを記憶している。

ルーティングテーブル６４１ｂは、図４３に示すように、複数のルート情報６４２ｂ、６４３ｂ・・・から構成される。各ルート情報は、アプリ番号、ホスト名、ＩＰアドレス、ポート番号及び処理状況から構成

される。アプリ番号、ホスト名、ＩＰアドレス及びポート番号は、上記のルーティングテーブル６４１に含まれるアプリ番号、ホスト名、ＩＰアドレス及びポート番号と同様であるので、説明を省略する。処理状況は、アプリ番号の示すアプリサーバ２００の処理状況を示している。処理状況「通常」は、アプリ番号の示すアプリサーバ２００が通常のサービス提供処理を行っていることを示す。処理状況「メンテナンス中」は、アプリ番号の示すアプリサーバ２００がメンテナンス中であることを示しており、管理サーバ６００は、処理状況「メンテナンス中」の場合、該当するアプリサーバ２００のパスワード変更の処理ができないことを判別する。

管理サーバ６００は、各アプリサーバ２００に定期的に監視信号を送信する。

各アプリサーバ２００は、管理サーバ６００から監視信号を受信し、自身の処理状態が通常であれば応答信号「通常」を返信する。自身の処理状況がメンテナンス中であれば応答信号「メンテナンス」を返信する。

管理サーバ６００は、各アプリサーバ２００から応答信号を受信し、受信した応答状況を基に、記憶しているルーティングデーブル６４１ｂの各アプリサーバ２００の処理状況を書き換える。

ユーザ端末又は内部ユーザ端末から、パスワード変更の要求を受信すると、管理サーバ６００は、ルーティングデーブル６４１ｂの処理状況を確認し、全てのアプリサーバ２００の処理状況が「通常」であると判断すると、上述したようなパスワード変更の処理を開始する。

処理状況が「通常」でないアプリサーバ２００が１つでも存在すれば、ユーザ端末へ、現在パスワードの変更を受け付けられない旨を通知する。

また、管理サーバ６００からの監視信号の有無にかかわらず、各アプリサーバ２００が自発的に、管理サーバ６００に自身の処理状況を報告するとしてもよい。

（７）アプリサーバによる現パスワードの記憶

実施の形態１～３において、管理サーバ６００がパスワード変更テー

ブル６５１により、現パスワードと新パスワードとを記憶しているが、各アプリサーバ２００が記憶しているとしてもよい。

この場合、管理サーバ６００は、第１アプリサーバ２００ａから第４アプリサーバ２００ｄの順に、ユーザＩＤと暗号化現パスワードと暗号化新パスワードとを送信し、パスワード変更を指示する。

各アプリサーバ２００は、ユーザＩＤと暗号化現パスワードと暗号化新パスワードと受信し、受信した暗号化現パスワードと暗号化新パスワードとを復号し、ユーザＩＤと現パスワードとを含むパスワード情報を選択し、選択したパスワード情報に含まれるパスワードを新パスワードに書き換える。書き換えが成功すれば、終了信号「１」を管理サーバへ送信する。次に、書き換えたパスワード情報に対応付けて、現パスワードを記憶しておく。

管理サーバ６００は、アプリサーバ２００から終了信号の受信し、受信した終了信号が「１」であれば、次のアプリサーバ２００へユーザＩＤと暗号化現パスワードと暗号化新パスワードとを送信する。

受信した終了信号が「０」である場合、又は一定時間を超えて終了信号を受信しない場合、パスワードの変更が失敗であると判断し、既に終了信号「１」を受信済みのアプリサーバ２００に、パスワード復旧の指示を送信する。

パスワード復旧の指示を受信したアプリサーバ２００は、書き換えたパスワード情報のパスワードを、記憶している現パスワードに書き換える。

（８）初期パスワードへの変更

実施の形態１～３において、利用者がパスワードを忘れている場合、パスワードを初期パスワードに変更するとしてもよい。

初期パスワードとは、パスワード変更システムの管理者側から利用者に最初に割り当てられるパスワードであり、メール、書面などで利用者に通達されるものである。一例として「００００」のような簡単な文字列やユーザＩＤと同じ文字列が挙げられる。

具体的には、管理サーバ６００は、あらかじめ各利用者の初期パスワードを記憶している。

ログイン画面１５１に、さらに、パスワード忘れボタンを設けておき、利用者は、パスワードを忘れた場合にパスワード忘れボタンを選択する。

ユーザ端末は、パスワード忘れボタンの押下を検出すると、管理サーバ６００へパスワード忘れを通知する。

管理サーバ６００は、ユーザ端末からパスワード忘れの通知を受信すると、叙述したようなパスワード変更の処理を開始する。このとき、利用者により入力された新パスワードに代わって初期パスワードを各アプリサーバ２００へ送信し、パスワードの変更を指示する。

全てのアプリサーバ２００のパスワード変更が成功すると、ユーザ端末へパスワードを初期パスワードに変更したことを通知する。

産業上の利用の可能性

本発明の各装置及びシステムは、各種のサービスをネットワークを介して、利用者に提供する産業において、経営的に、また継続的及び反復的に使用することができる。また、本発明を構成する各装置、コンピュータプログラム及び記録媒体は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。

請 求 の 範 囲

1．一のパスワードにより認証した一の利用者へ各サービスを提供する複数のアプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置であって、

全てのアプリケーション装置のパスワードの更新を試みる第１手段と、

各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第２手段と、

不可能と判断されるアプリケーション装置が少なくとも１台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第３手段と

を備えることを特徴とする管理サーバ装置。

2．前記管理サーバ装置は、さらに、

利用者装置からパスワードの更新の要求を受信する第４手段を含み、

前記第１手段は、受信した前記更新の要求に基づいて、パスワードの更新を試みる

ことを特徴とする請求の範囲１に記載の管理サーバ装置。

3．前記第１手段は、全てのアプリケーション装置に対してパスワードの更新を指示し、

前記第２手段は、各アプリケーション装置について、パスワードの更新が失敗したか否かを判断し、

前記第３手段は、少なくとも１台のアプリケーション装置について、更新が失敗したと判断される場合に、パスワードの更新が成功した他のアプリケーション装置に対して、更新前のパスワードへの復元を指示する

ことを特徴とする請求の範囲２に記載の管理サーバ装置。

4．前記第４手段は、利用者の新パスワードと旧パスワードとを含む前記更新の要求を受信し、

前記第１手段は、受信した更新の要求に含まれる新パスワードと旧パ

スワードとを含む更新の指示を生成し、生成した前記更新の指示を全てのアプリケーション装置に対して送信する

ことを特徴とする請求の範囲３に記載の管理サーバ装置。

５．前記第２手段は、

各アプリケーション装置からのパスワードの更新の成功又は失敗を示す応答を受信する応答受信部と、

受信した前記応答が成功を示す場合に、当該アプリケーション装置についてパスワードの更新が成功したと断定し、受信した前記応答が失敗を示す場合に、当該アプリケーション装置についてパスワードの更新が失敗したと断定する断定部と

を含むことを特徴とする請求の範囲３に記載の管理サーバ装置。

６．前記第２手段は、

時間の経過に伴って経過時間を計測する計時部と、

前記第１手段による更新の指示の送信の時点において、計時部により計測される経過時間を初期値にリセットする初期化部と、

各アプリケーション装置からのパスワードの更新の成功又は失敗を示す応答を待ち受ける待受部と、

計測された経過時間が、所定のしきい値より大きいか否かを判断する判断部と、

判断部により経過時間が前記しきい値と等しいか又は小さいと判断され、かつ待受部により各アプリケーション装置からの応答を受信し、かつその応答が成功を示す場合に、当該アプリケーション装置について、パスワードの更新が成功したと断定し、その他の場合に、当該アプリケーション装置について、パスワードの更新が失敗したと断定する断定部と

を含むことを特徴とする請求の範囲３に記載の管理サーバ装置。

７．前記第１手段は、全てのアプリケーション装置に対してパスワードの更新の準備を指示し、

前記第２手段は、各アプリケーション装置について、パスワードの更

新の準備が未完了か否かを判断し、

前記第３手段は、少なくとも１台のアプリケーション装置について、更新の準備が未完了と判断される場合に、更新の準備が完了した他のアプリケーション装置に対して、前記更新の準備の指示を取り消す

ことを特徴とする請求の範囲２に記載の管理サーバ装置。

８．前記第４手段は、利用者の新パスワードと旧パスワードとを含む前記更新の要求を受信し、

前記第１手段は、受信した更新の要求に含まれる新パスワードと旧パスワードとを含む更新の準備の指示を生成し、生成した前記更新の準備の指示を全てのアプリケーション装置に対して送信する

ことを特徴とする請求の範囲７に記載の管理サーバ装置。

９．前記第２手段は、

アプリケーション装置からのパスワードの更新の準備の完了又は未完了を示す応答を受信する応答受信部と、

受信した前記応答が完了を示す場合に、当該アプリケーション装置についてパスワードの更新の準備が完了したと断定し、受信した前記応答が未完了を示す場合に、当該アプリケーション装置についてパスワードの更新の準備が未完了であると断定する断定部と

を含むことを特徴とする請求の範囲７に記載の管理サーバ装置。

１０．前記第２手段は、

時間の経過に伴って経過時間を計測する計時部と、

前記第１手段による更新の準備の指示の送信の時点において、計時部により計測される経過時間を初期値にリセットする初期化部と、

アプリケーション装置からのパスワードの更新の準備の完了又は未完了を示す応答を待ち受ける待受部と、

計測された経過時間が、所定のしきい値より大きいか否かを判断する判断部と、

判断部により経過時間が前記しきい値と等しいか又は小さいと判断され、かつ待受部によりアプリケーション装置からの応答を受信し、かつ

その応答が完了を示す場合に、パスワードの更新の準備が完了したと断定し、その他の場合に、パスワードの更新の準備が未完了であると断定する断定部と

を含むことを特徴とする請求の範囲７に記載の管理サーバ装置。

１１．前記管理サーバ装置は、さらに、

前記第２手段によりパスワードの更新が不可能と判断される場合に、元のパスワードに戻す旨のメッセージを前記利用者装置へ送信するメッセージ送信手段

を含むことを特徴とする請求の範囲２に記載の管理サーバ装置。

１２．前記管理サーバ装置は、さらに、

各アプリケーション装置について、メインテナンス中であるか否かを記憶している管理記憶手段を備え、

前記第１手段は、メインテナンス中のアプリケーション装置が存在しない場合に、パスワードの更新を試みる

ことを特徴とする請求の範囲２に記載の管理サーバ装置。

１３．前記第１手段は、メインテナンス中のアプリケーション装置が存在する場合に、パスワードの更新を中止し、

前記管理サーバ装置は、さらに、

前記第１手段によりパスワードの更新が中止される場合に、パスワードの更新を中止する旨のメッセージを前記利用者装置へ送信するメッセージ送信手段を含む

ことを特徴とする請求の範囲２に記載の管理サーバ装置。

１４．前記アプリケーション装置は、第１ネットワークを介して、前記管理サーバ装置と接続されており、

前記利用者装置は、第１ネットワークに接続されていない第２ネットワークを介して、前記管理サーバ装置と接続されている

ことを特徴とする請求の範囲２に記載の管理サーバ装置。

１５．前記第１ネットワーク及び前記第２ネットワークは、イントラネットである

ことを特徴とする請求の範囲１４に記載の管理サーバ装置。

１６．前記管理サーバ装置と、各アプリケーション装置とは、専用線を介して、接続されており、

パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、各アプリケーション装置との間で、パスワードの更新のための情報を送受信し、

各サービスの提供の際には、前記管理サーバ装置は、第１及び第２ネットワークを介して、前記利用者装置と各アプリケーション装置との間で、前記サービスに係る情報の送受信を中継する

ことを特徴とする請求の範囲１４に記載の管理サーバ装置。

１７．前記アプリケーション装置及び前記利用者装置は、ネットワークを介して、前記管理サーバ装置と接続されており、

前記管理サーバ装置は、さらに、

アプリケーションの種類と、各アプリケーション装置のネットワーク上における位置情報とを対応付ける対応テーブルを記憶している記憶手段と、

前記利用者装置から、アプリケーションを示す種類情報と処理の内容を示す処理情報とを受信する受信手段と、

前記対応テーブルを用いて、受信した種類情報に対応するアプリケーション装置の位置情報を取得する取得手段と、

取得した位置情報により示されるアプリケーション装置に対して、前記処理情報を送信する送信手段と

を含むことを特徴とする請求の範囲２に記載の管理サーバ装置。

１８．前記ネットワークは、インターネットである

ことを特徴とする請求の範囲１６に記載の管理サーバ装置。

１９．更新後の新パスワードは、利用者に最初に割り当てられた初期パスワードであり、

前記第１手段は、全てのアプリケーション装置の初期パスワードへの更新を試み、

前記第２手段は、各アプリケーション装置について、初期パスワードへの更新が不可能か否かを判断し、

前記第３手段は、不可能と判断されるアプリケーション装置が少なくとも１台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする

ことを特徴とする請求の範囲１に記載の管理サーバ装置。

２０．一のパスワードにより認証した一の利用者へサービスを提供し、管理サーバ装置からの指示によりパスワードを更新するアプリケーション装置であって、

更新前のパスワードを記憶している旧パスワード記憶手段と、

利用者の認証に用いるパスワードを記憶している認証用パスワード記憶手段と、

管理サーバ装置から、パスワードを更新前のものに復元する復元指示を受信する受信手段と、

前記復元指示を受信すると、旧パスワード記憶手段から更新前のパスワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きする書込手段と

を備えることを特徴とするアプリケーション装置。

２１．前記アプリケーション装置は、前記管理サーバ装置を介して、利用者の利用者装置との間で、前記サービスに関する情報の送受信を行う

ことを特徴とする請求の範囲２０に記載のアプリケーション装置。

２２．前記アプリケーション装置は、メインテナンス中である場合に、当該旨を前記管理サーバ装置に対して通知する

ことを特徴とする請求の範囲２１に記載のアプリケーション装置。

２３．前記アプリケーション装置は、第１ネットワークを介して、前記管理サーバ装置と接続されており、

前記利用者装置は、第１ネットワークに接続されていない第２ネットワークを介して、前記管理サーバ装置と接続されている

ことを特徴とする請求の範囲２１に記載のアプリケーション装置。

２４．前記アプリケーション装置及び前記管理サーバ装置は、専用線を介して接続されており、

パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、前記管理サーバとの間で、パスワードの更新のための情報を送受信し、

各サービスの提供の際には、第１及び第２ネットワークを介して、前記サービスに係る情報を送受信する

ことを特徴とする請求の範囲２３に記載のアプリケーション装置。

２５．前記アプリケーション装置及び前記利用者装置は、インターネットを介して、前記管理サーバ装置と接続されている

ことを特徴とする請求の範囲２１に記載のアプリケーション装置。

２６．利用者の端末装置と、一のパスワードにより認証した一の利用者の端末装置へ各サービスを提供する複数のアプリケーション装置と、前記アプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置とから構成されるパスワード更新システムであって、

前記管理サーバ装置は、

全てのアプリケーション装置のパスワードの更新を試みる第１手段と、

各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第２手段と、

不可能と判断されるアプリケーション装置が少なくとも１台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第３手段とを備え、

各アプリケーション装置は、

更新前のパスワードを記憶している旧パスワード記憶手段と、

利用者の認証に用いるパスワードを記憶している認証用パスワード記憶手段と、

管理サーバ装置から、パスワードを更新前のものに復元する復元指示を受信する受信手段と、

前記復元指示を受信すると、旧パスワード記憶手段から更新前のパス

ワードを読み出し、読み出したパスワードを認証用パスワード記憶手段に上書きする書込手段とを備える

ことを特徴とするパスワード更新システム。

２７．前記端末装置と各アプリケーション装置とは、前記管理サーバ装置を介して、情報の送受信を行う

ことを特徴とする請求の範囲２６に記載のパスワード更新システム。

２８．前記アプリケーション装置は、第１ネットワークを介して、前記管理サーバ装置と接続されており、

前記利用者装置は、第１ネットワークに接続されていない第２ネットワークを介して、前記管理サーバ装置と接続されている

ことを特徴とする請求の範囲２７に記載のパスワード更新システム。

２９．前記第１ネットワーク及び前記第２ネットワークは、イントラネットである

ことを特徴とする請求の範囲２８に記載のパスワード更新システム。

３０．前記管理サーバ装置と、各アプリケーション装置とは、専用回線を介して、接続されており、

パスワードの更新の際には、前記管理サーバ装置は、前記専用線を介して、前記管理サーバとの間で、パスワードの更新のための情報を送受信し、

各サービスの提供の際には、第１及び第２ネットワークを介して、前記サービスに係る情報を送受信する

ことを特徴とする請求の範囲２８に記載のパスワード更新システム。

３１．前記アプリケーション装置及び前記利用者装置は、ネットワークを介して、前記管理サーバ装置と接続されており、

前記管理サーバ装置は、さらに、

アプリケーションの種類と、各アプリケーション装置のネットワーク上における位置情報とを対応付ける対応テーブルを記憶している記憶手段と、

前記利用者装置から、アプリケーションを示す種類情報と処理の内容

を示す処理情報とを受信する受信手段と、

前記対応テーブルを用いて、受信した種類情報に対応するアプリケーション装置の位置情報を取得する取得手段と、

取得した位置情報により示されるアプリケーション装置に対して、前記処理情報を送信する送信手段と

を含むことを特徴とする請求の範囲２７に記載のパスワード更新システム。

３２．前記ネットワークは、インターネットである

ことを特徴とする請求の範囲３０に記載のパスワード更新システム。

３３．一のパスワードにより認証した一の利用者へ各サービスを提供する複数のアプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置で用いられる管理サーバ制御方法であって、

全てのアプリケーション装置のパスワードの更新を試みる第１ステップと、

各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第２ステップと、

不可能と判断されるアプリケーション装置が少なくとも１台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとする第３ステップと

を含むことを特徴とする管理サーバ制御方法。

３４．一のパスワードにより認証した一の利用者へ各サービスを提供する複数のアプリケーション装置に対して、当該パスワードの更新を指示する管理サーバ装置で用いられる管理サーバ制御プログラムであって、

全てのアプリケーション装置のパスワードの更新を試みる第１ステップと、

各アプリケーション装置について、パスワードの更新が不可能か否かを判断する第２ステップと、

不可能と判断されるアプリケーション装置が少なくとも１台存在する場合に、全てのアプリケーション装置のパスワードを更新前のものとす

る第３ステップと

を含むことを特徴とする管理サーバ制御プログラム。

３５．前記管理サーバ制御プログラムは、

コンピュータ読み取り可能なプログラム記録媒体に記録されている

ことを特徴とする請求の範囲３４に記載の管理サーバ制御プログラム。

図1

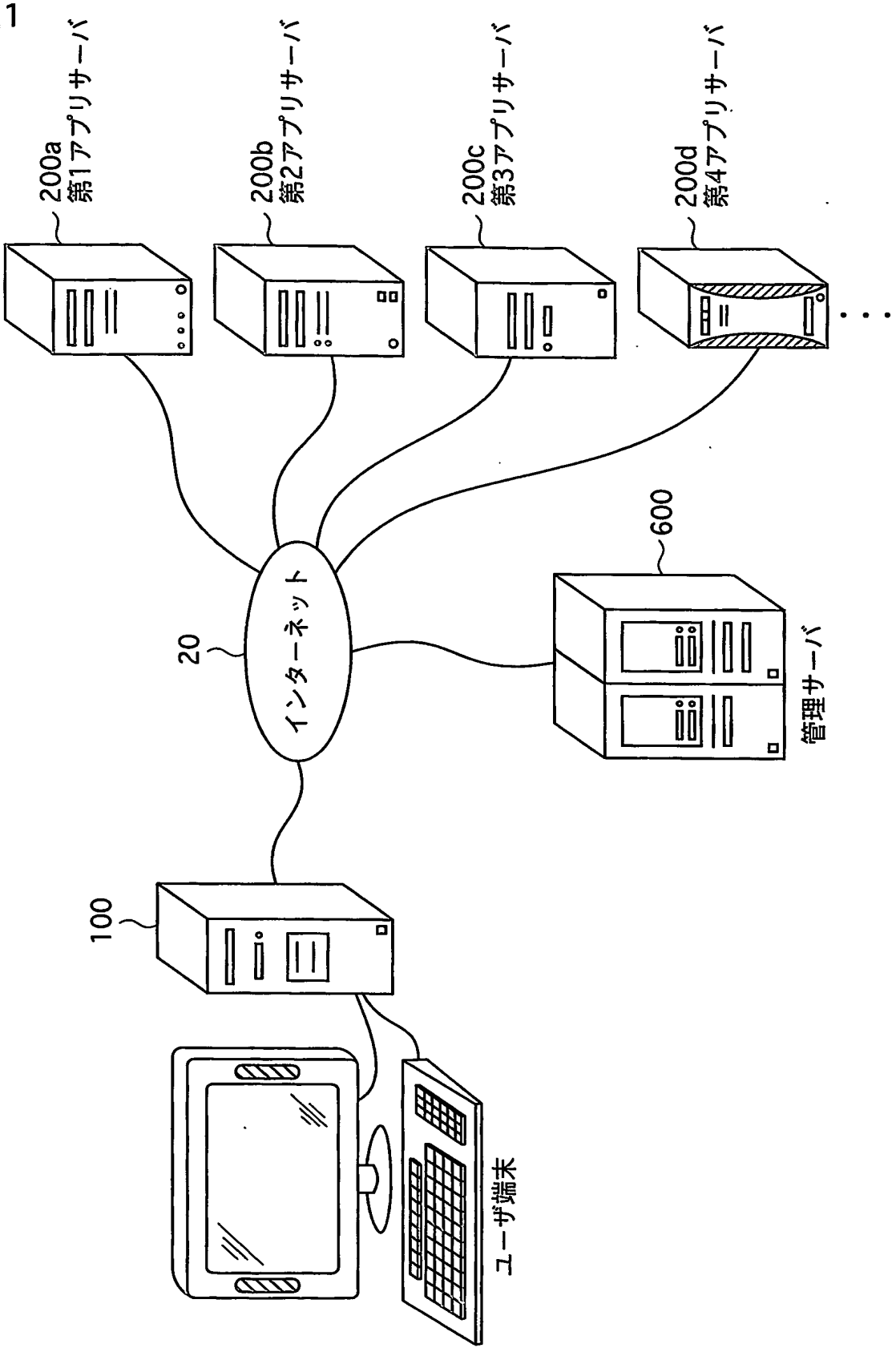

200a
第1アプリサーバ
200b
第2アプリサーバ
200c
第3アプリサーバ
200d
第4アプリサーバ
600
管理サーバ
20
インターネット
100
ユーザ端末

図2

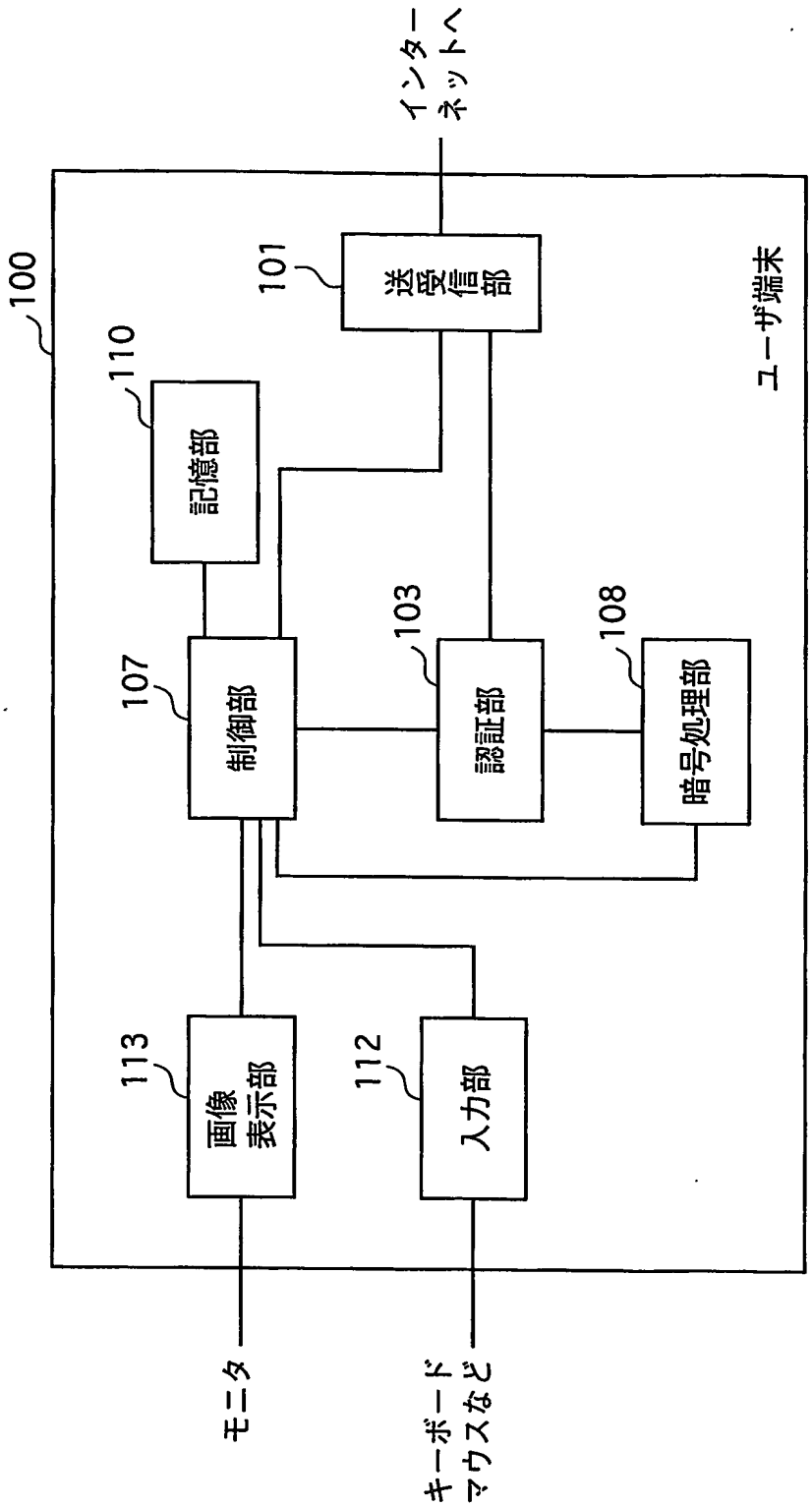

インターネットへ
100
101
送受信部
ユーザ端末
110
記憶部
103
108
107
制御部
認証部
暗号処理部
113
画像表示部
112
入力部
モニタ
キーボード
マウスなど

図3

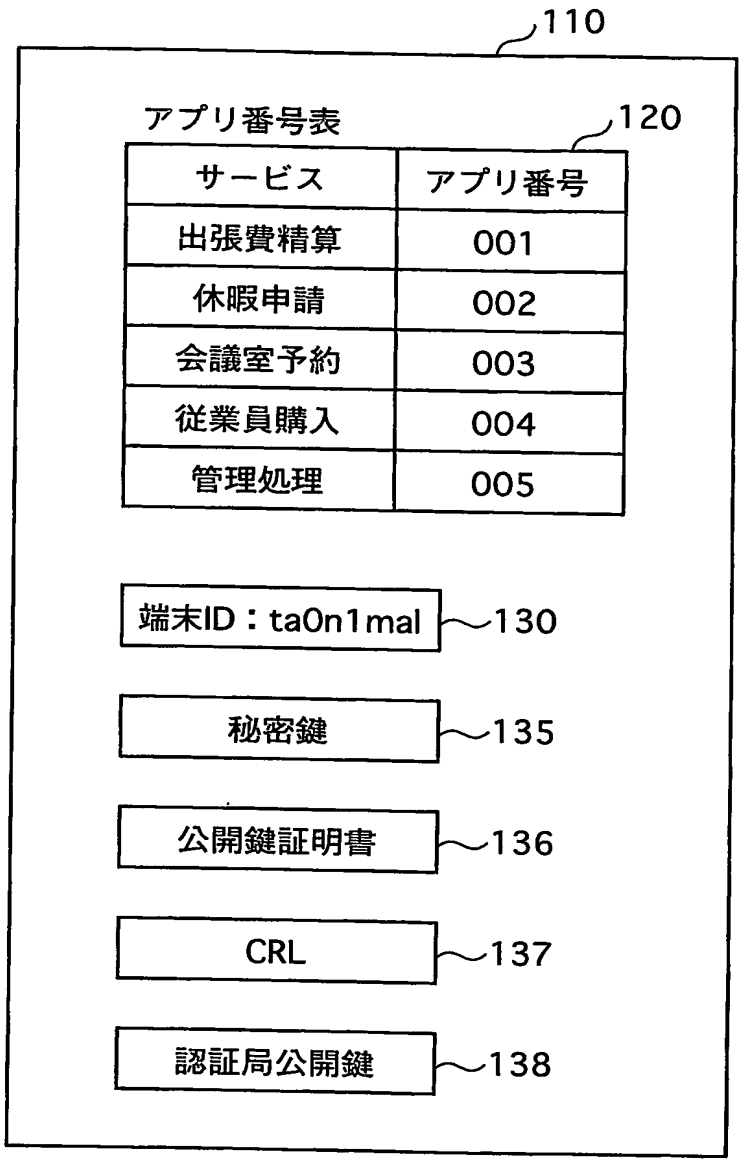
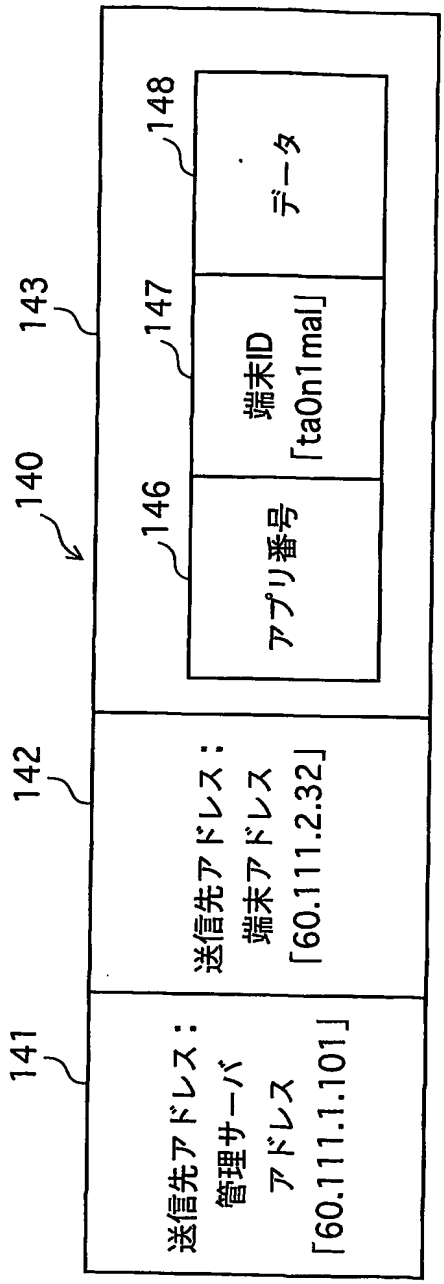

110
アプリ番号表
120
サービス
アプリ番号
出張費精算
001
休暇申請
002
会議室予約
003
従業員購入
004
管理処理
005
端末ID：ta0n1mal
130
秘密鍵
135
公開鍵証明書
136
CRL
137
認証局公開鍵
138

図4


141
送信先アドレス：
管理サーバ
アドレス
「60.111.1.101」
142
送信先アドレス：
端末アドレス
「60.111.2.32」
140
143
146
アプリ番号
147
端末ID
「ta0n1mal」
148
データ

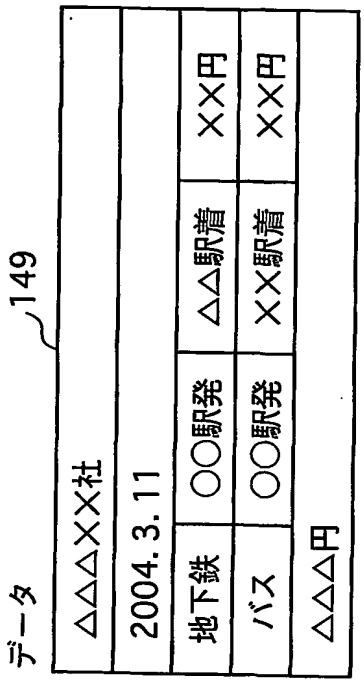

データ
149
△△△XX社
2004. 3. 11
地下鉄
○○駅発
△△駅着
XX円
バス
○○駅発
XX駅着
XX円
△△△円

図5

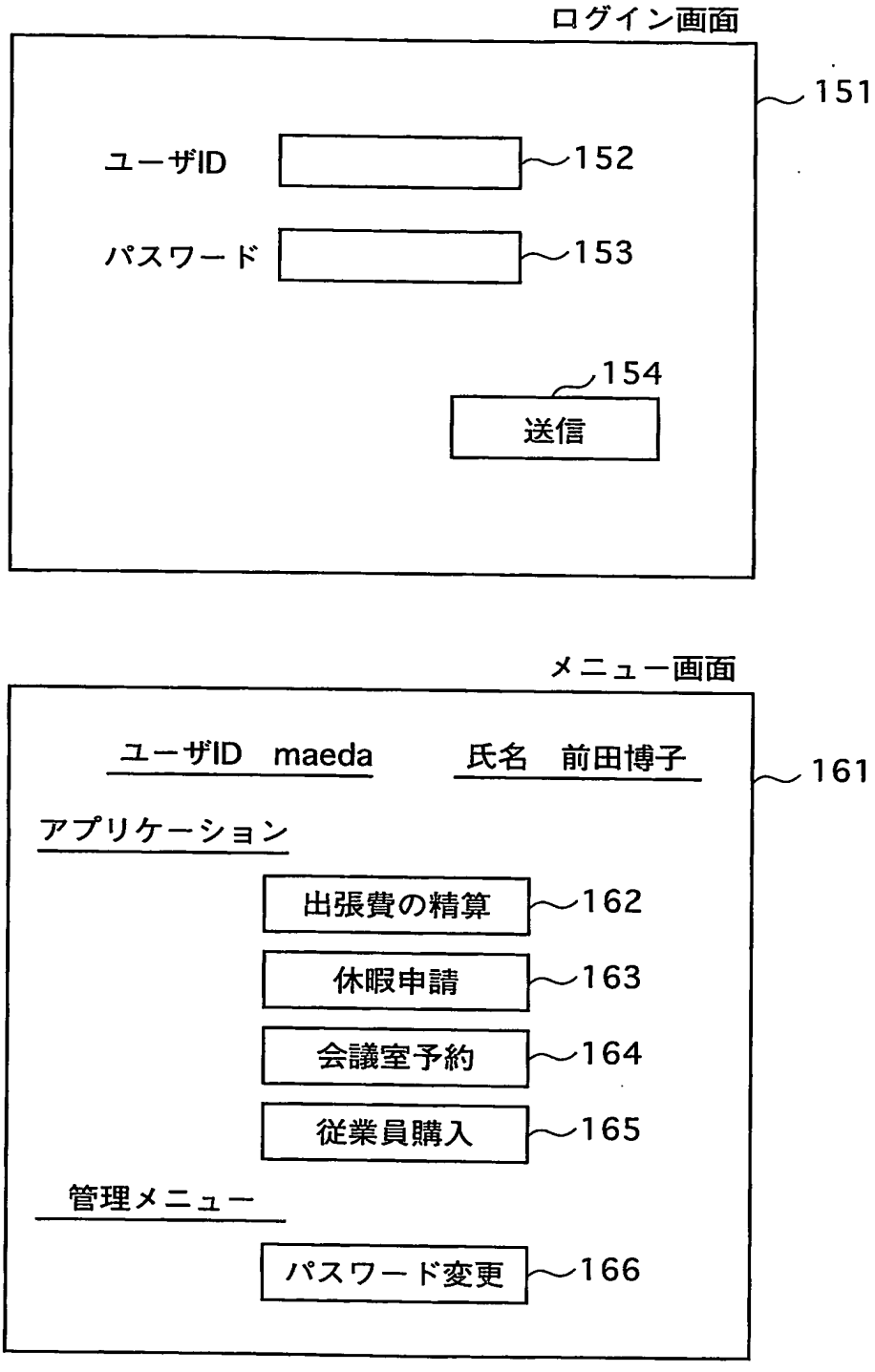

ログイン画面
151
ユーザID
152
パスワード
153
154
送信
メニュー画面
ユーザID maeda
氏名 前田博子
161
アプリケーション
出張費の精算
162
休暇申請
163
会議室予約
164
従業員購入
165
管理メニュー
パスワード変更
166

図6

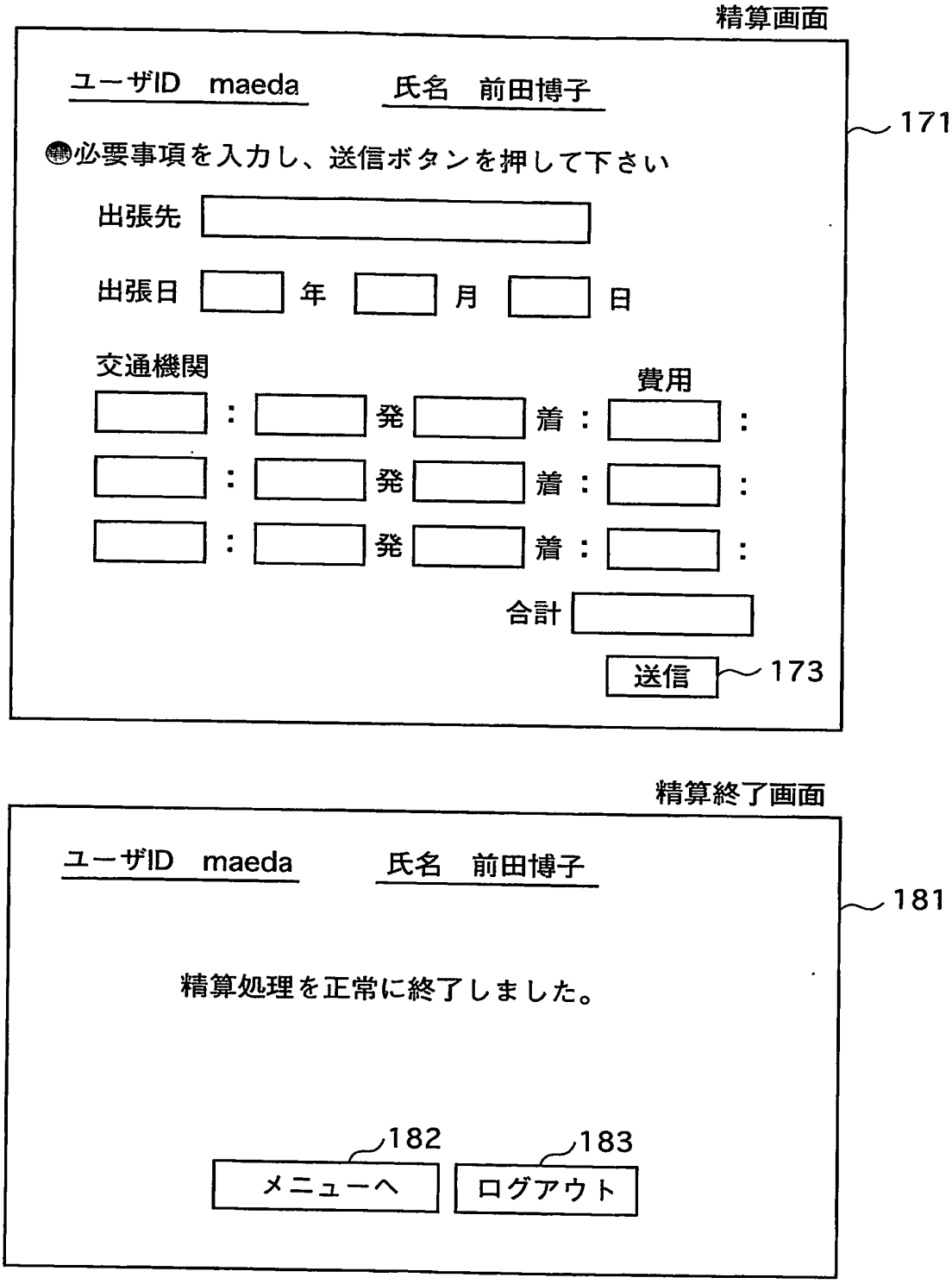

精算画面
ユーザID maeda
氏名 前田博子
171
必要事項を入力し、送信ボタンを押して下さい
出張先
出張日
年
月
日
交通機関
費用
発
着
合計
送信
173
精算終了画面
ユーザID maeda
氏名 前田博子
181
精算処理を正常に終了しました。
182
183
メニューへ
ログアウト

図7

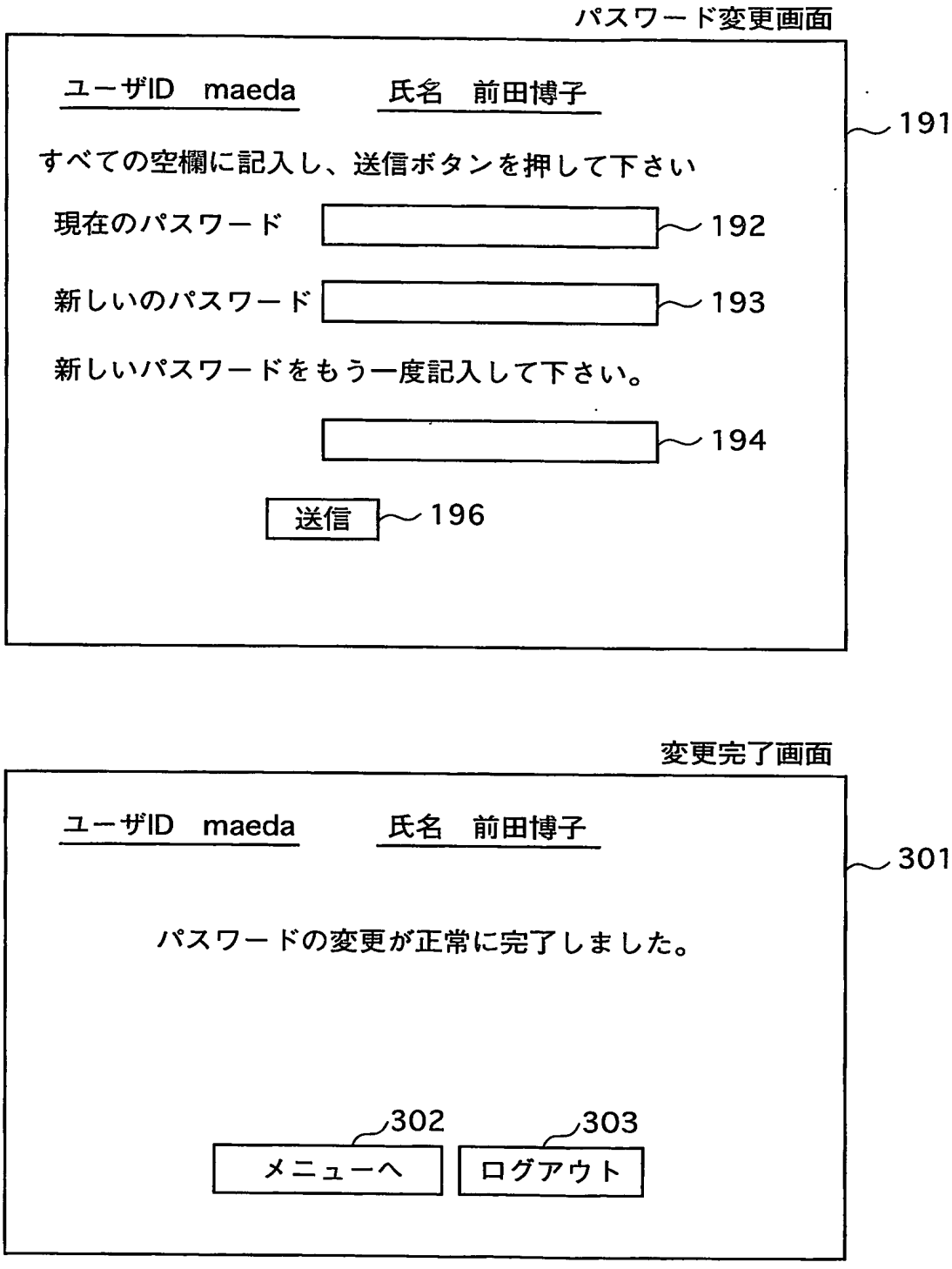

パスワード変更画面
ユーザID maeda
氏名 前田博子
191
すべての空欄に記入し、送信ボタンを押して下さい
現在のパスワード
192
新しいのパスワード
193
新しいパスワードをもう一度記入して下さい。
194
送信
196
変更完了画面
ユーザID maeda
氏名 前田博子
301
パスワードの変更が正常に完了しました。
302
303
メニューへ
ログアウト

図8

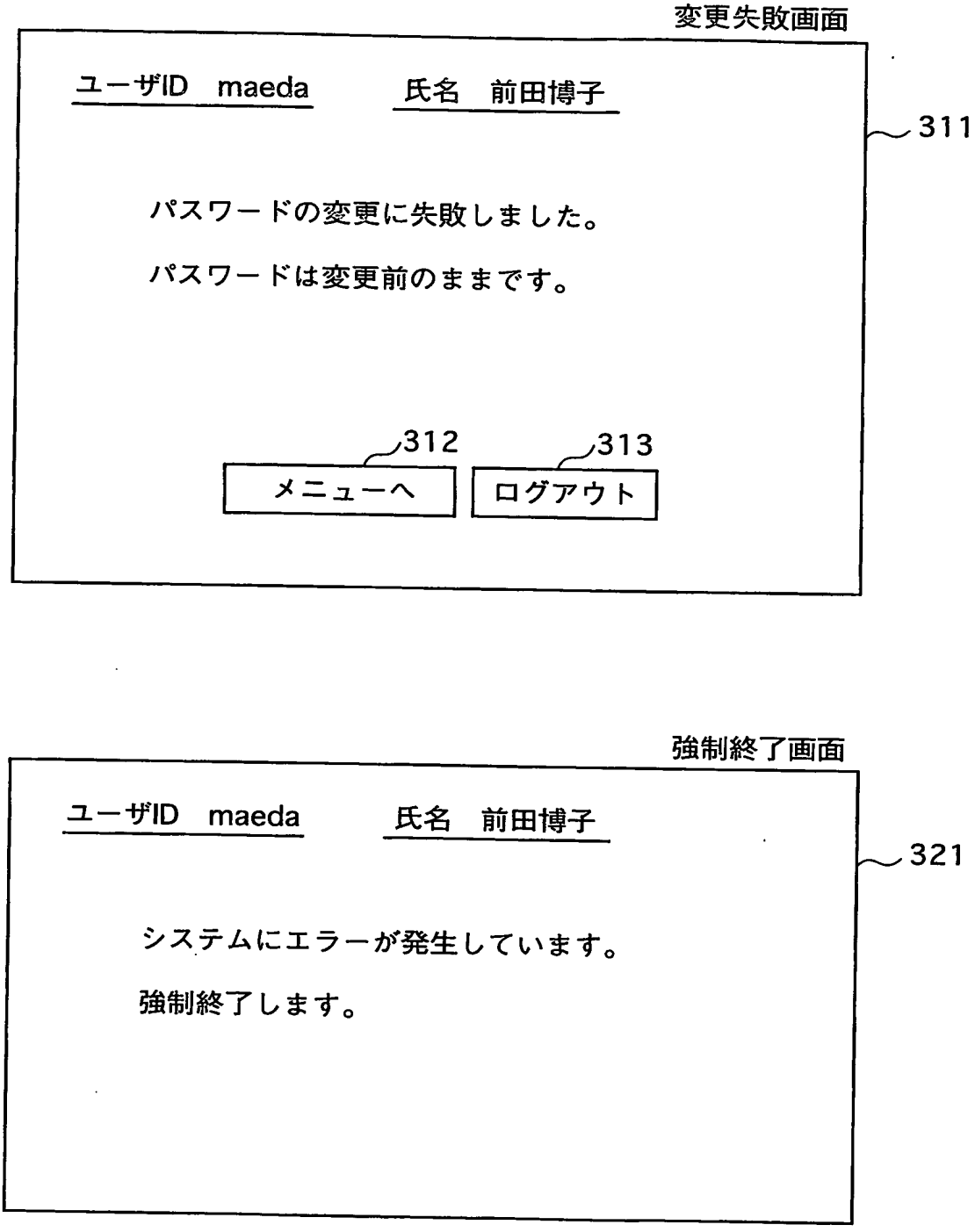

変更失敗画面
ユーザID maeda
氏名 前田博子
311
パスワードの変更に失敗しました。
パスワードは変更前のままです。
312
313
メニューへ
ログアウト
強制終了画面
ユーザID maeda
氏名 前田博子
321
システムにエラーが発生しています。
強制終了します。

図9

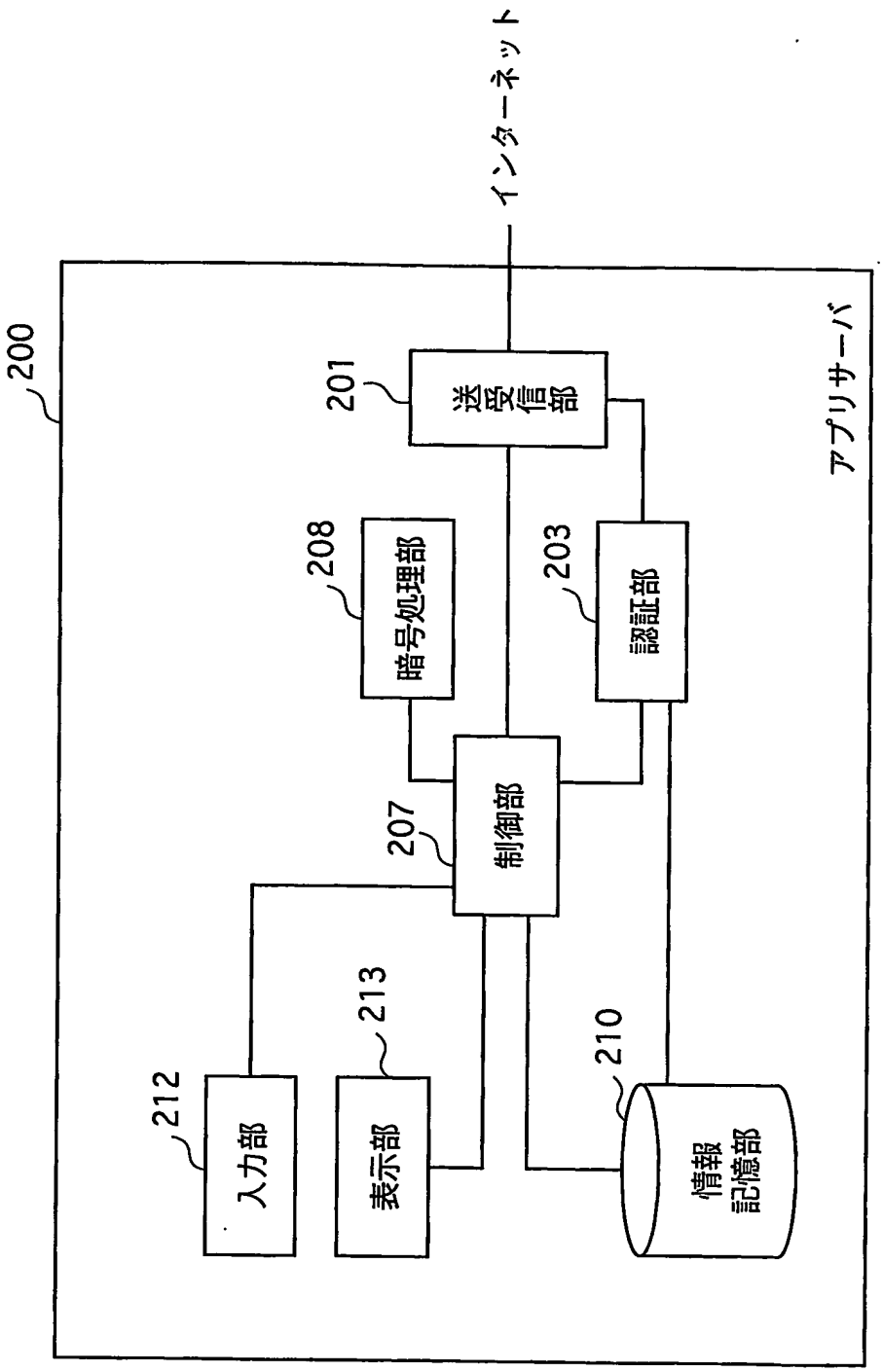

インターネット
200
アプリサーバ
201
送受信部
208
暗号処理部
203
認証部
207
制御部
212
入力部
213
表示部
210
情報
記憶部

図10

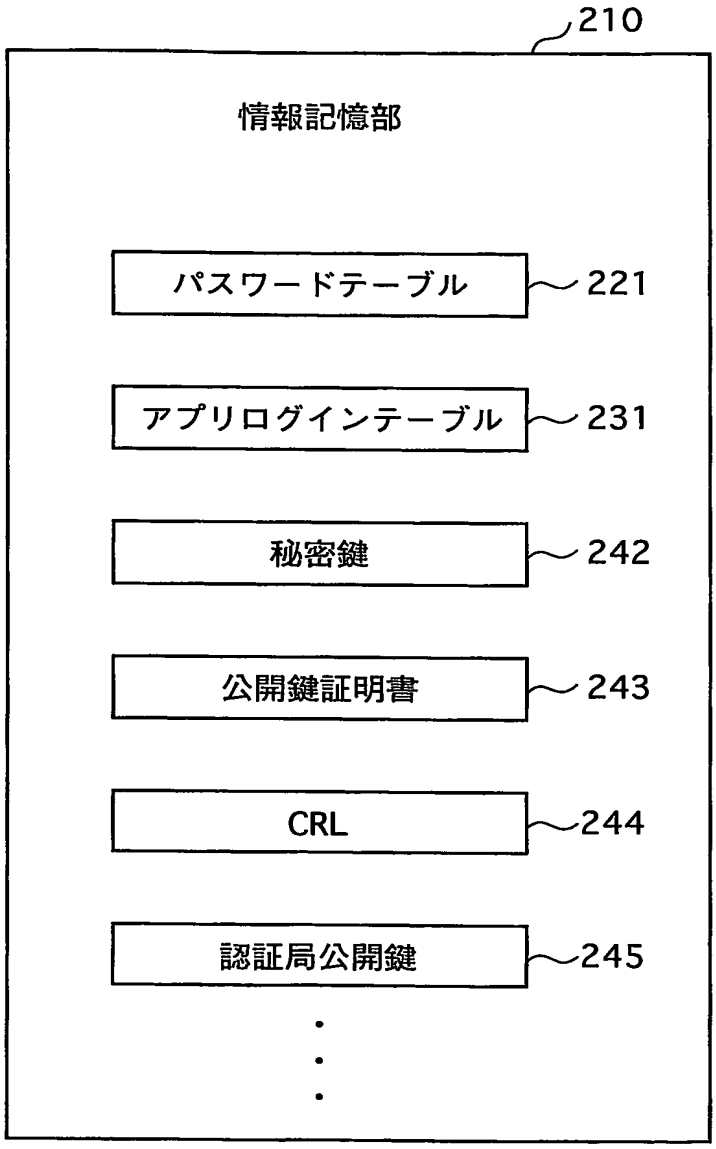

210
情報記憶部
パスワードテーブル
221
アプリログインテーブル
231
秘密鍵
242
公開鍵証明書
243
CRL
244
認証局公開鍵
245

図11

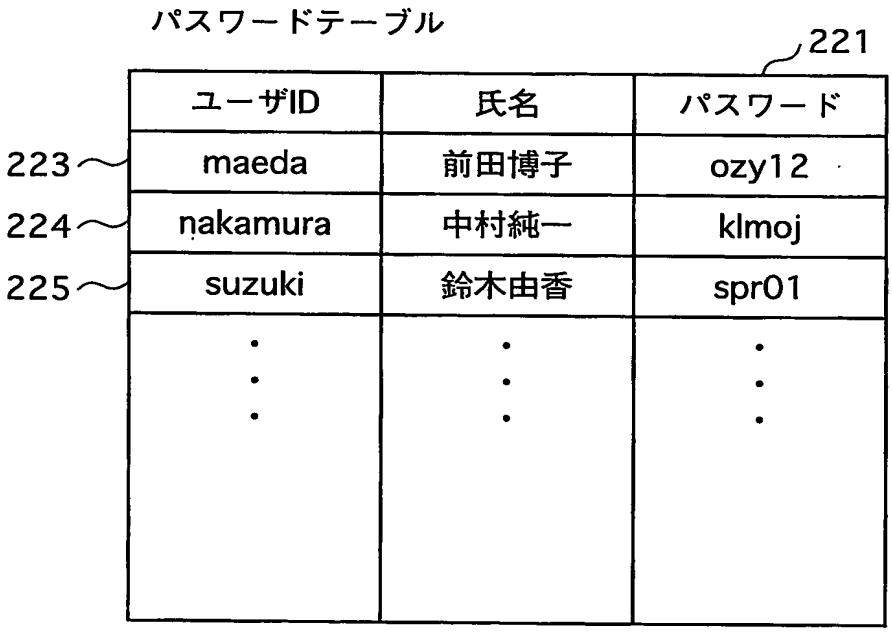

パスワードテーブル
221
ユーザID
氏名
パスワード
223
maeda
前田博子
ozy12
224
nakamura
中村純一
klmoj
225
suzuki
鈴木由香
spr01

図12

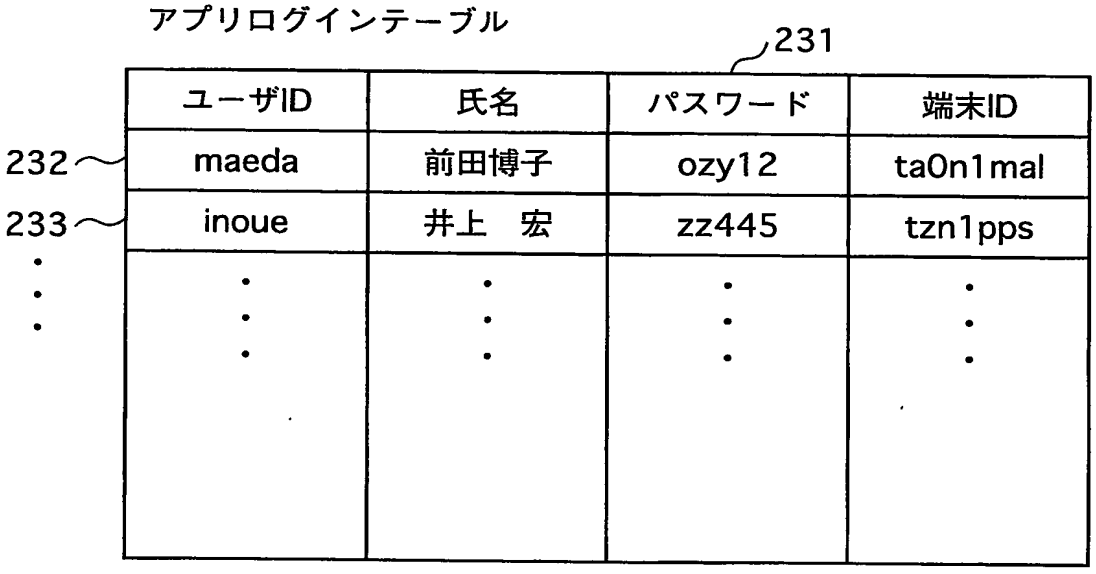

アプリログインテーブル
231
ユーザID
氏名
パスワード
端末ID
232
maeda
前田博子
ozy12
ta0n1mal
233
inoue
井上　宏
zz445
tzn1pps

図13

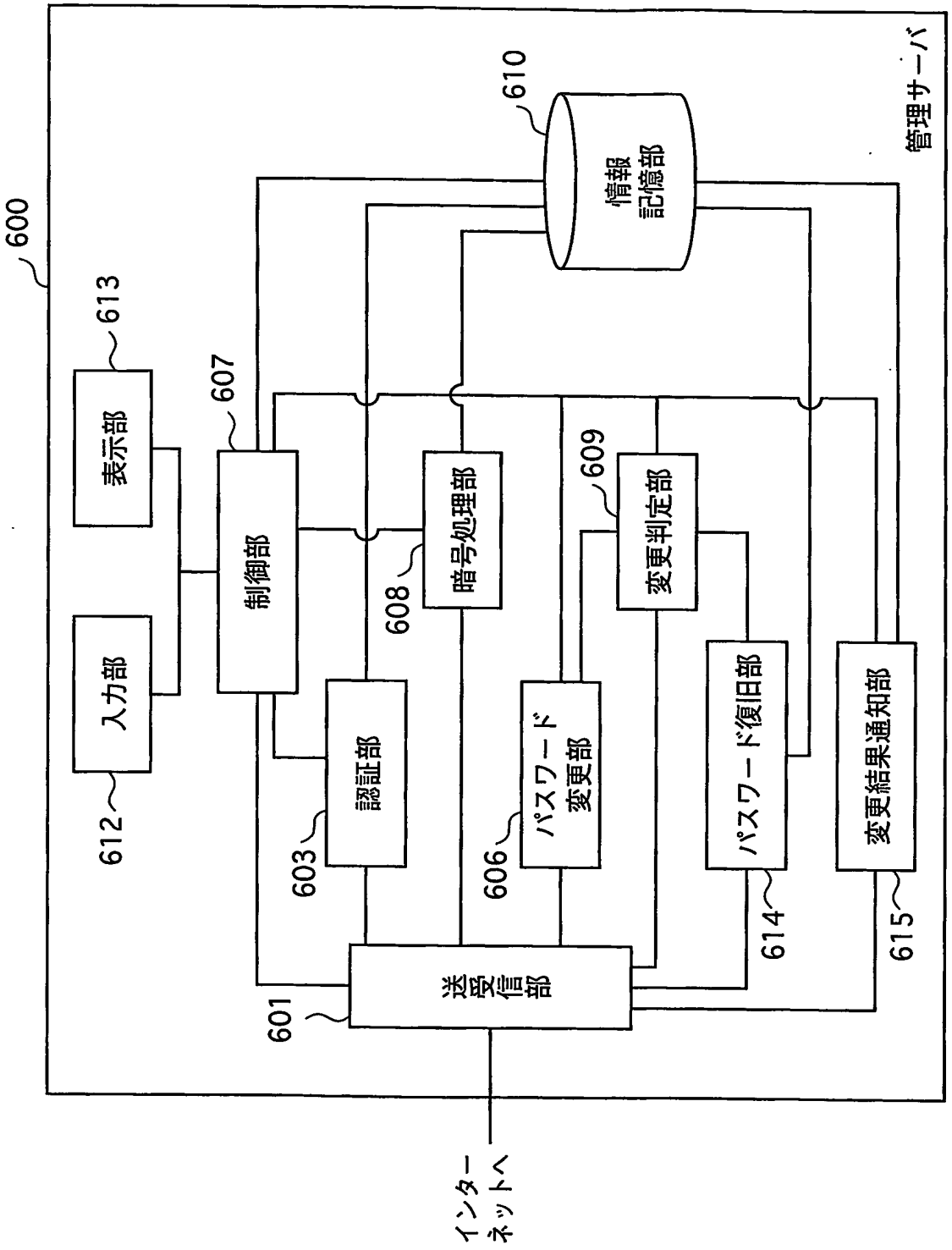

管理サーバ
600
610
情報記憶部
613
表示部
607
制御部
609
変更判定部
608
暗号処理部
入力部
612
603
認証部
606
パスワード変更部
パスワード復旧部
614
変更結果通知部
615
601
送受信部
インターネットへ

図14

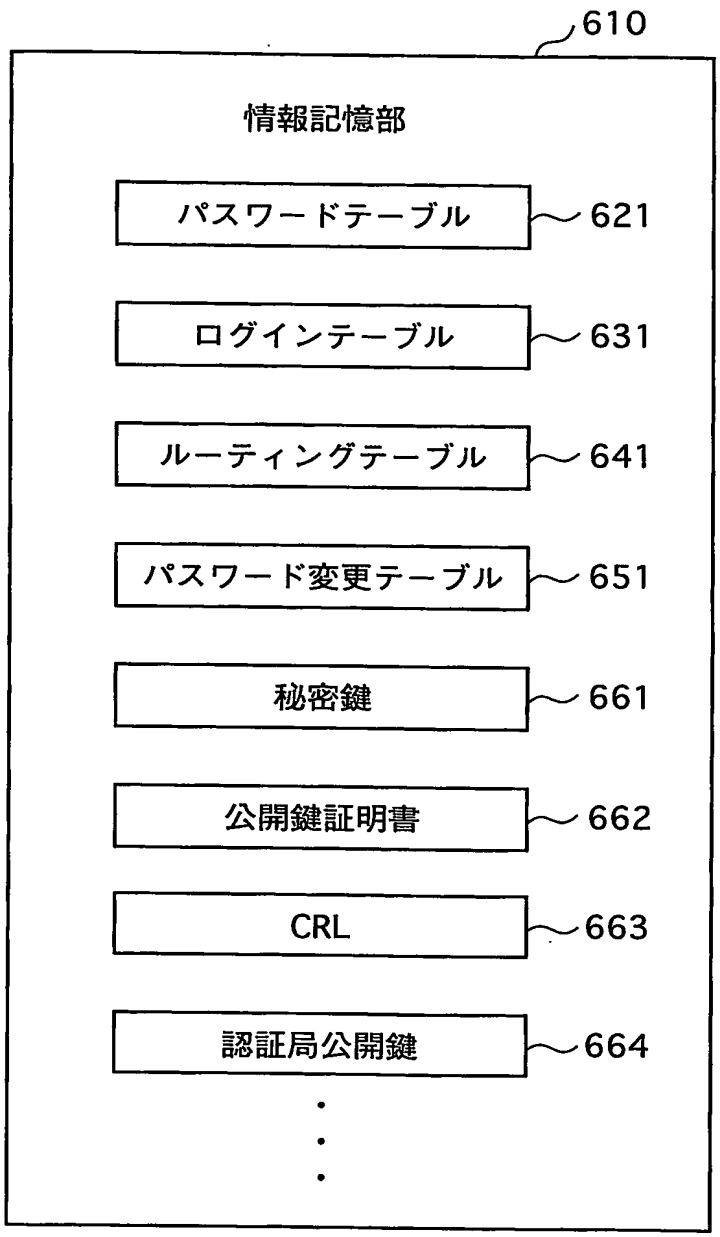

610
情報記憶部
パスワードテーブル
621
ログインテーブル
631
ルーティングテーブル
641
パスワード変更テーブル
651
秘密鍵
661
公開鍵証明書
662
CRL
663
認証局公開鍵
664

図15

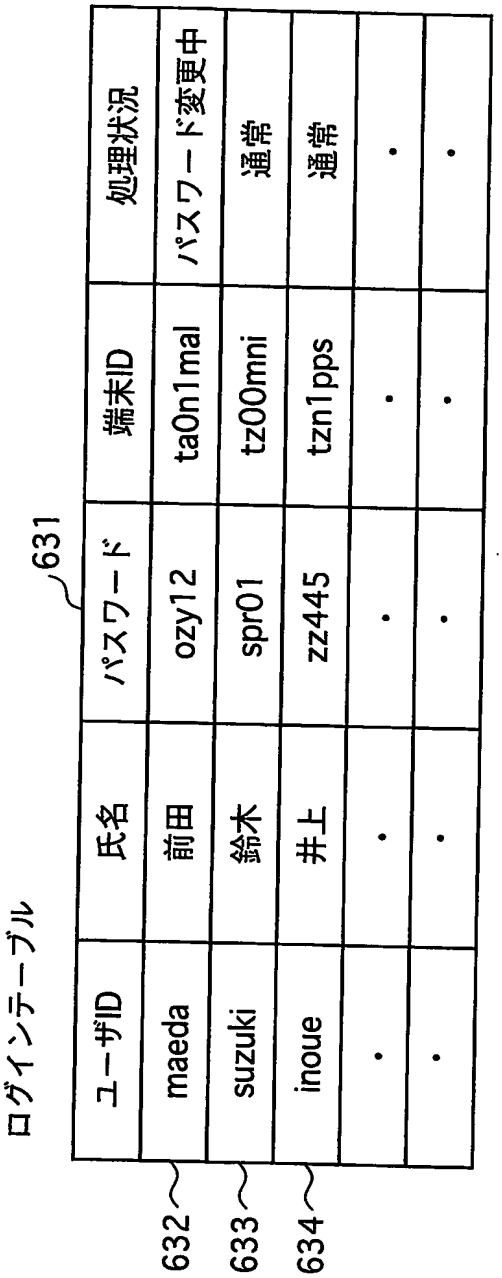

ログインテーブル
631
632
633
634
ユーザID
氏名
パスワード
端末ID
処理状況
maeda
前田
ozy12
ta0n1mal
パスワード変更中
suzuki
鈴木
spr01
tz00mni
通常
inoue
井上
zz445
tzn1pps
通常

図16

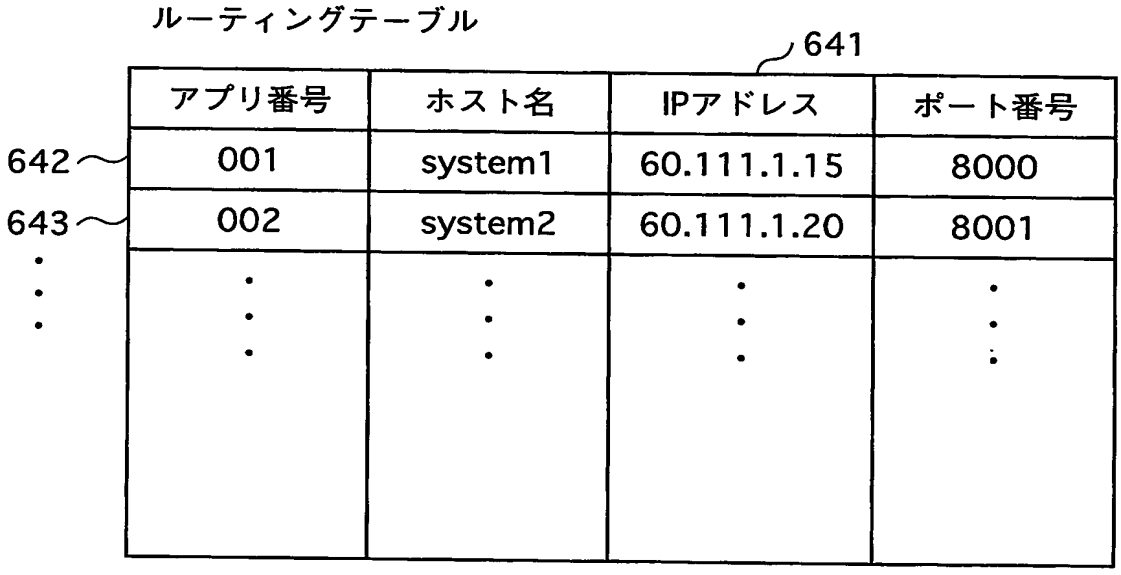

ルーティングテーブル
641
642
643
アプリ番号
ホスト名
IPアドレス
ポート番号
001
system1
60.111.1.15
8000
002
system2
60.111.1.20
8001

図17

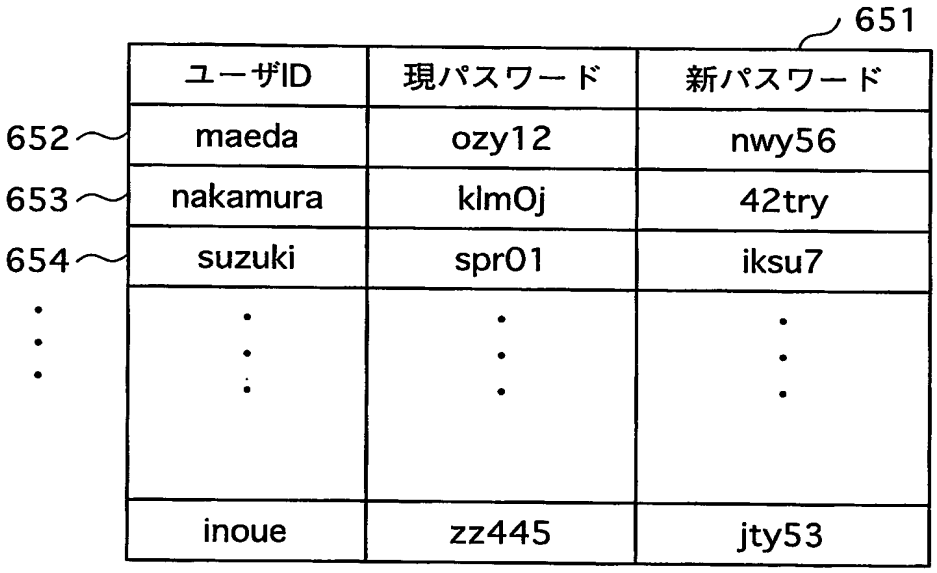

651
ユーザID
現パスワード
新パスワード
652
maeda
ozy12
nwy56
653
nakamura
klmOj
42try
654
suzuki
spr01
iksu7
inoue
zz445
jty53

図18

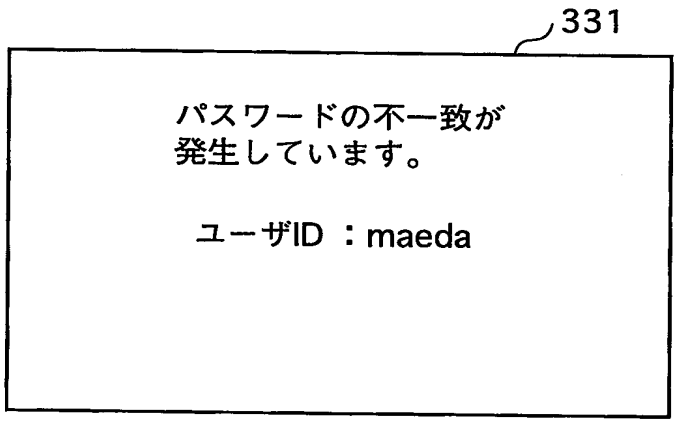


図19

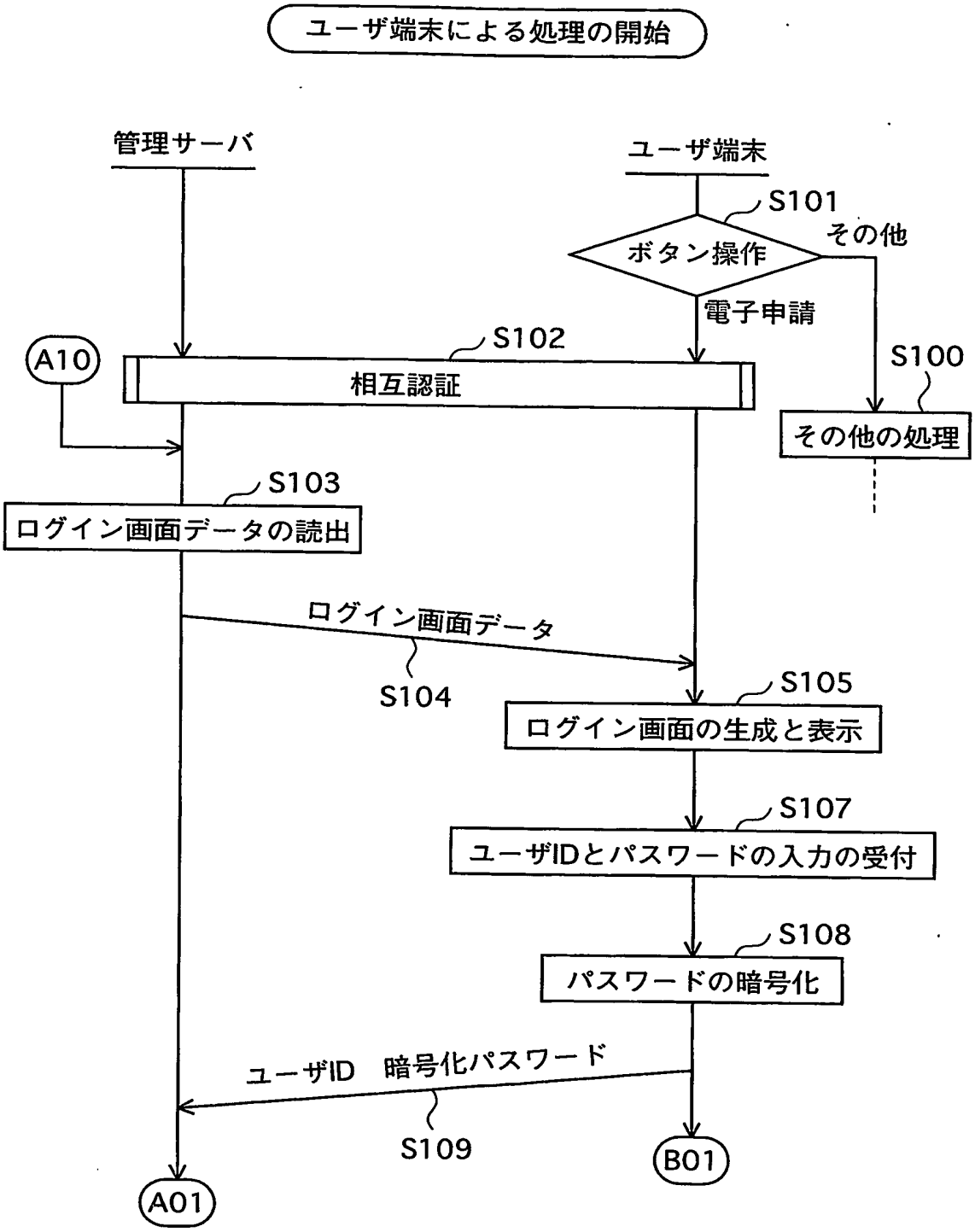

ユーザ端末による処理の開始
管理サーバ
ユーザ端末
S101
ボタン操作
その他
電子申請
A10
S102
相互認証
S100
その他の処理
S103
ログイン画面データの読出
ログイン画面データ
S104
S105
ログイン画面の生成と表示
S107
ユーザIDとパスワードの入力の受付
S108
パスワードの暗号化
ユーザID 暗号化パスワード
S109
B01
A01

図20

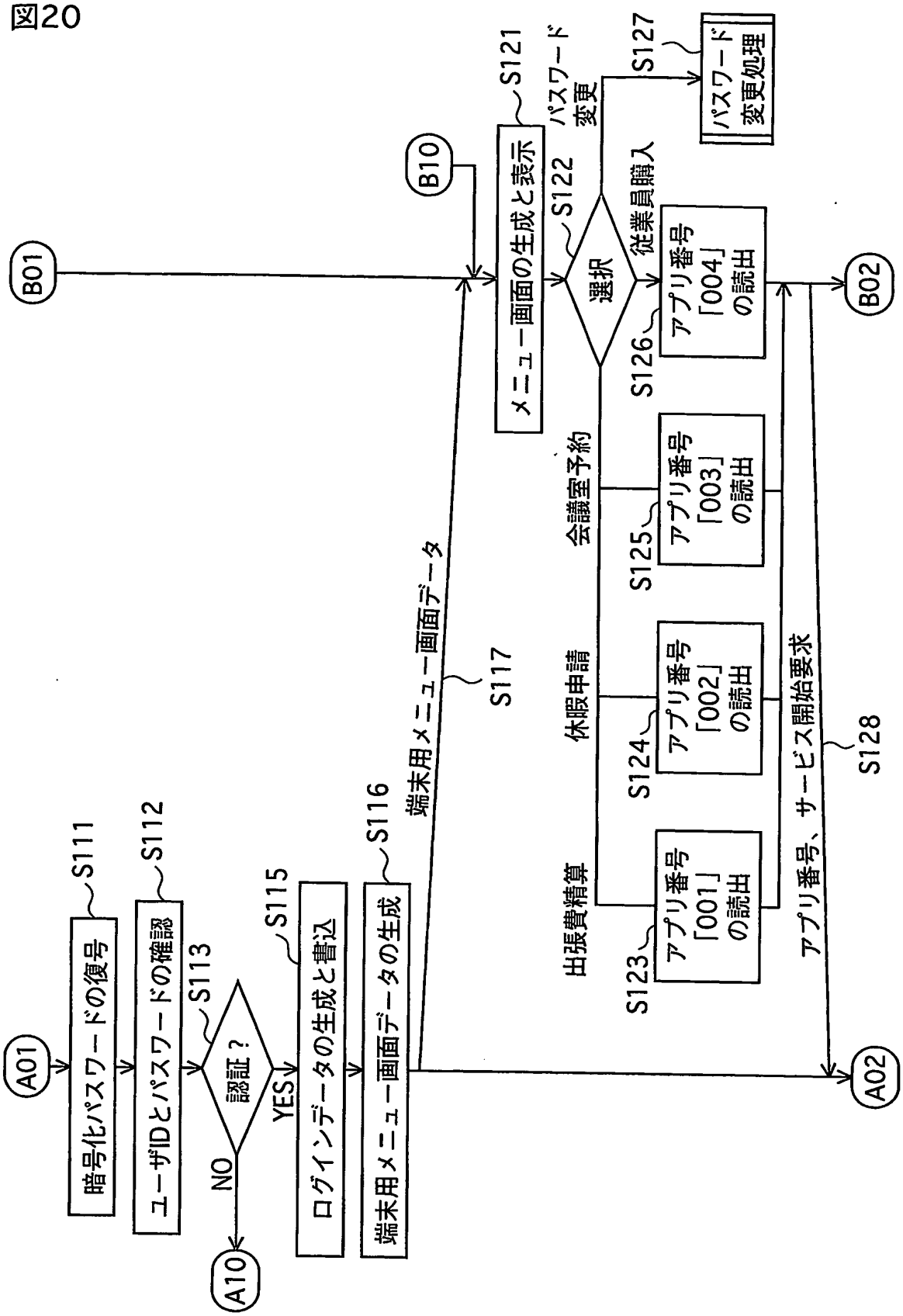

A01
暗号化パスワードの復号
S111
ユーザIDとパスワードの確認
S112
認証？
S113
NO
A10
YES
ログインデータの生成と書込
S115
端末用メニュー画面データの生成
S116
端末用メニュー画面データ
S117
B01
B10
メニュー画面の生成と表示
S121
選択
S122
出張費精算
アプリ番号「001」の読出
S123
休暇申請
アプリ番号「002」の読出
S124
会議室予約
アプリ番号「003」の読出
S125
従業員購入
アプリ番号「004」の読出
S126
パスワード変更
パスワード変更処理
S127
アプリ番号、サービス開始要求
S128
B02
A02

図21

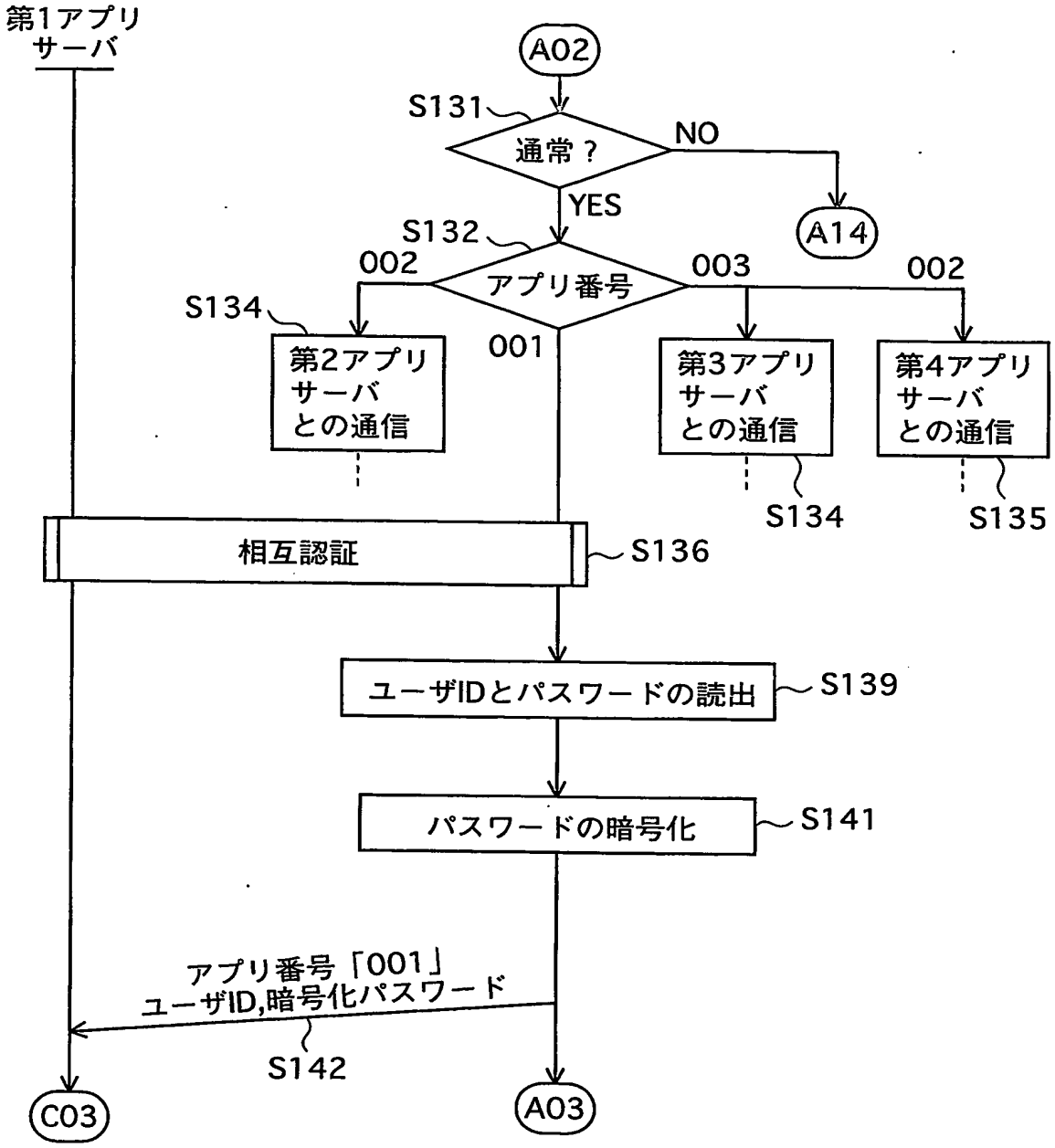

第1アプリ
サーバ
A02
S131
通常？
NO
YES
A14
S132
002
アプリ番号
003
002
S134
001
第2アプリ
サーバ
との通信
第3アプリ
サーバ
との通信
第4アプリ
サーバ
との通信
S134
S135
相互認証
S136
ユーザIDとパスワードの読出
S139
パスワードの暗号化
S141
アプリ番号「001」
ユーザID,暗号化パスワード
S142
C03
A03

図22

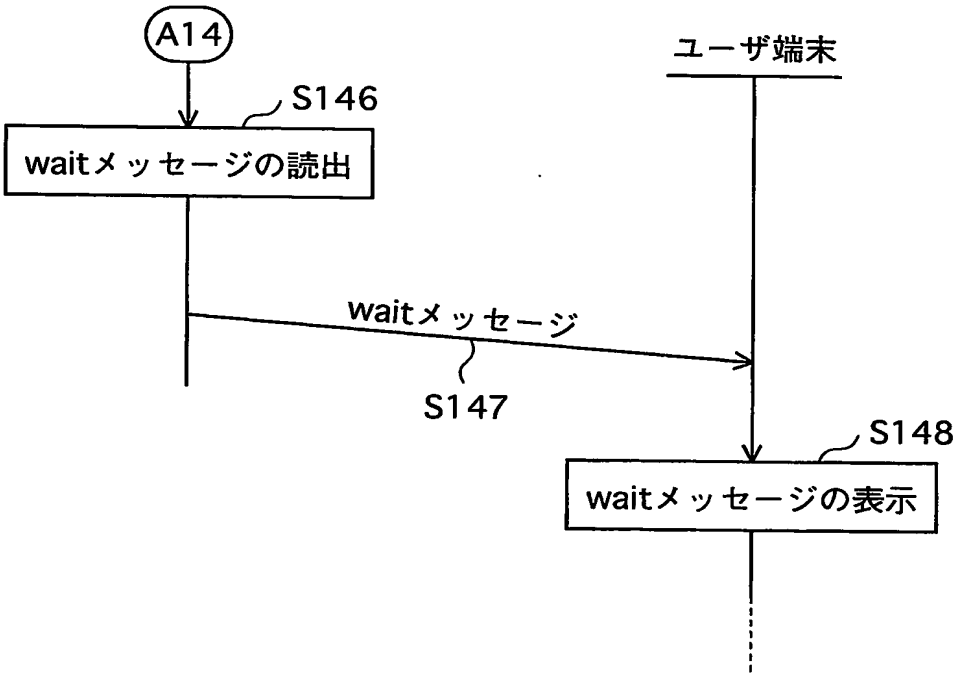

A14
ユーザ端末
S146
waitメッセージの読出
waitメッセージ
S147
S148
waitメッセージの表示

図23

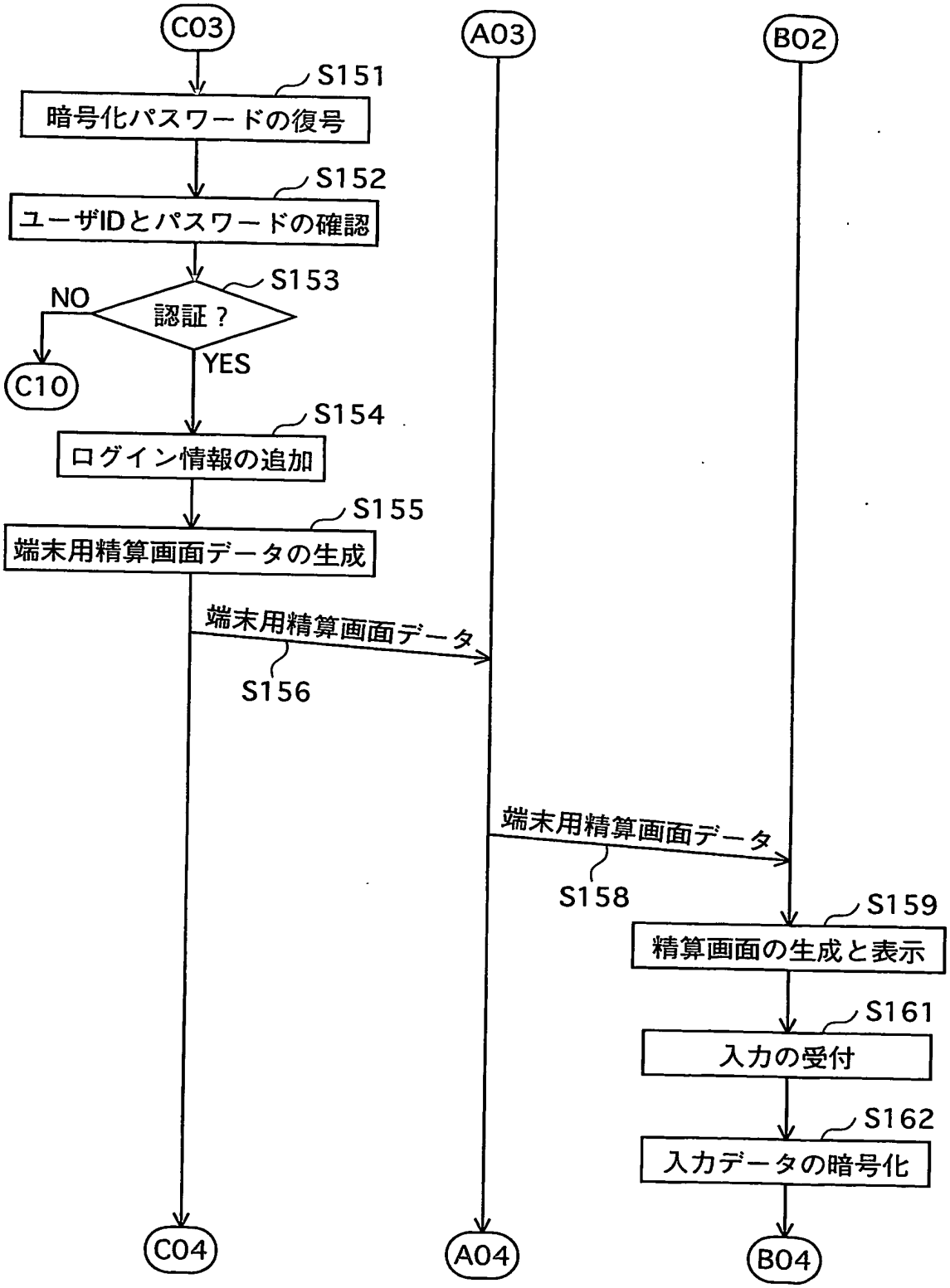

C03
A03
B02
S151
暗号化パスワードの復号
S152
ユーザIDとパスワードの確認
S153
認証？
NO
YES
C10
S154
ログイン情報の追加
S155
端末用精算画面データの生成
端末用精算画面データ
S156
端末用精算画面データ
S158
S159
精算画面の生成と表示
S161
入力の受付
S162
入力データの暗号化
C04
A04
B04

図24

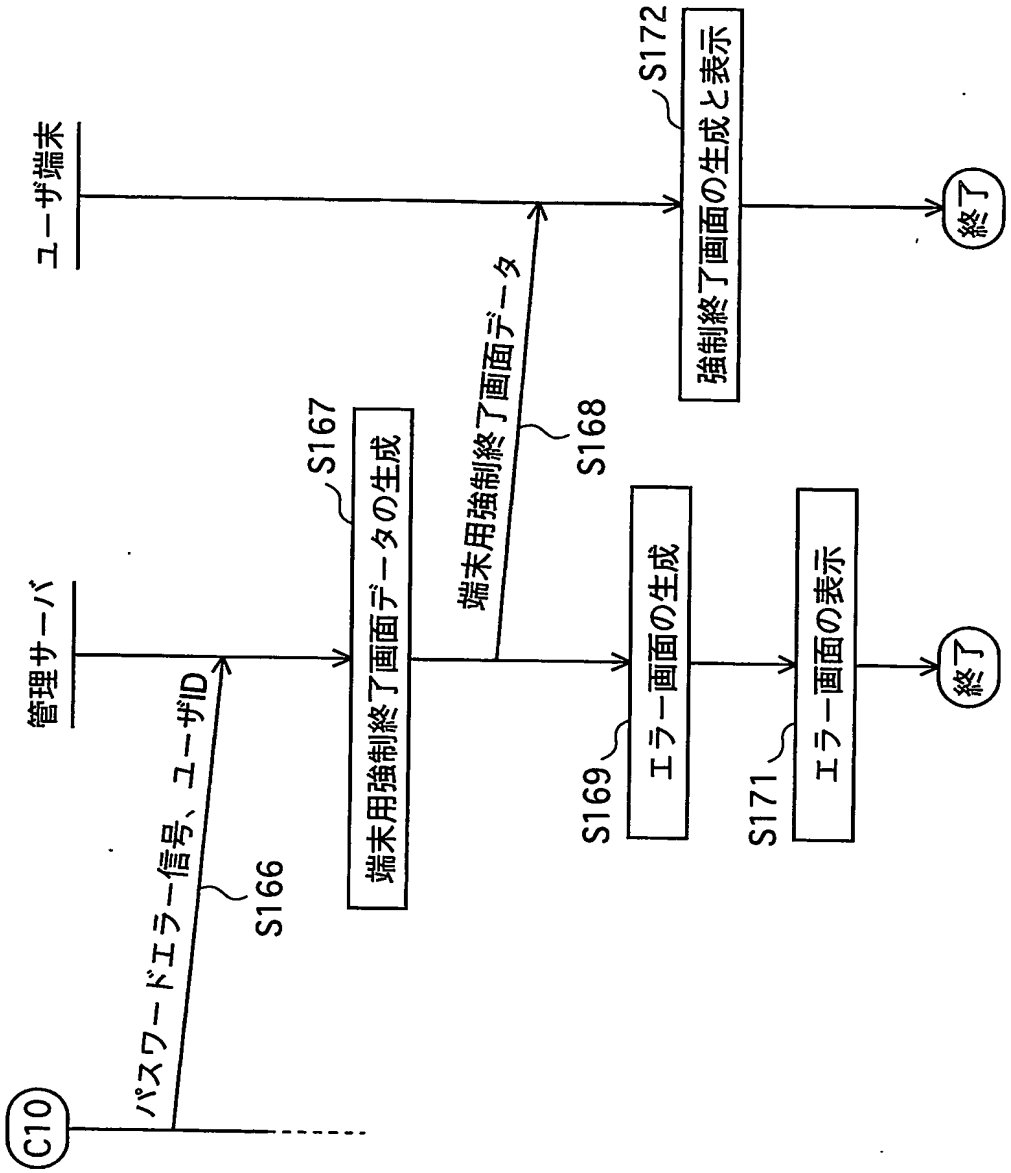

ユーザ端末
管理サーバ
C10
パスワードエラー信号、ユーザID
S166
端末用強制終了画面データの生成
S167
端末用強制終了画面データ
S168
エラー画面の生成
S169
エラー画面の表示
S171
強制終了画面の生成と表示
S172
終了
終了

図25

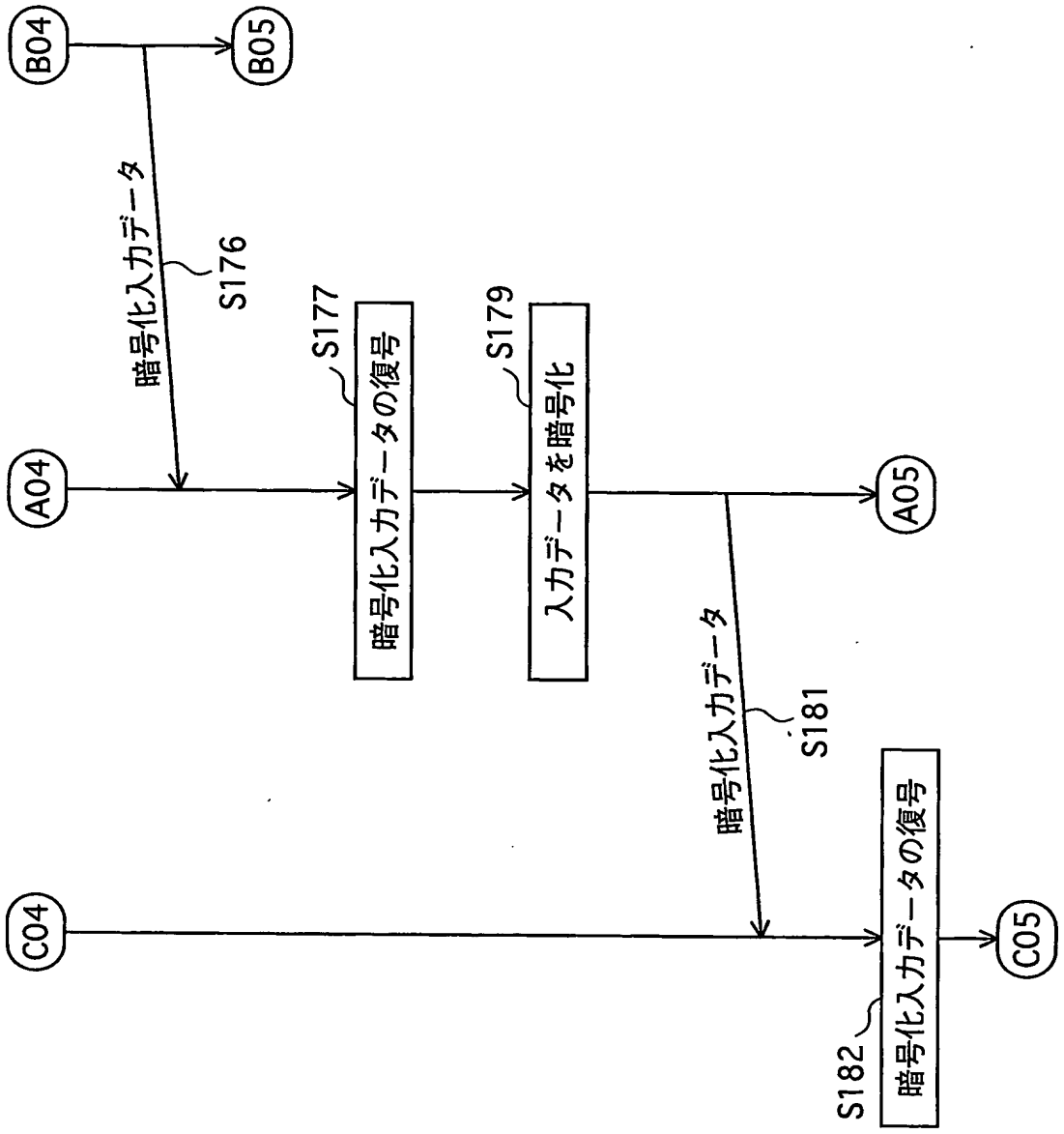

B04
B05
暗号化入力データ
S176
S177
暗号化入力データの復号
S179
入力データを暗号化
A04
A05
暗号化入力データ
S181
C04
C05
S182
暗号化入力データの復号

図26

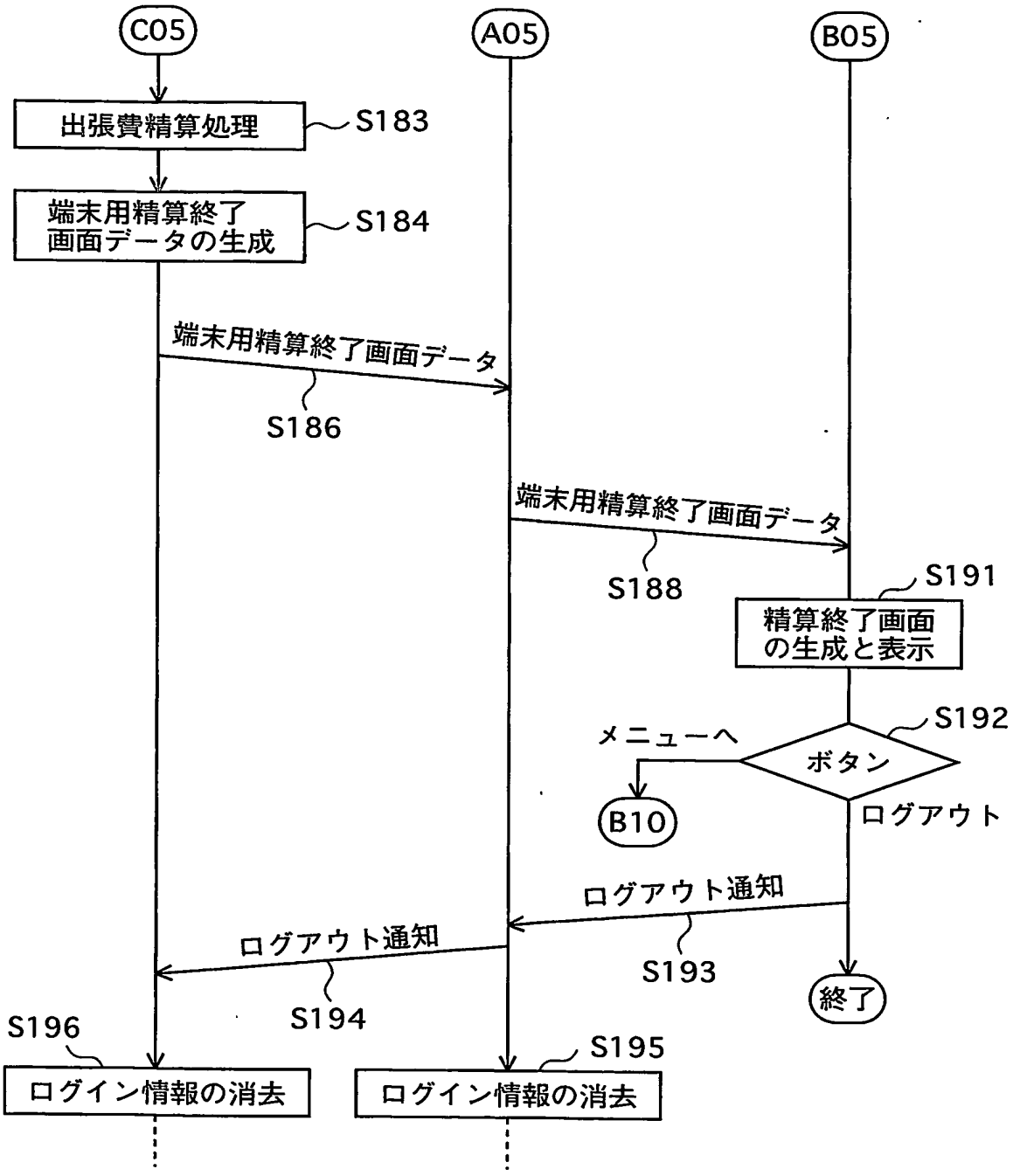

C05
A05
B05
出張費精算処理
S183
端末用精算終了
画面データの生成
S184
端末用精算終了画面データ
S186
端末用精算終了画面データ
S188
S191
精算終了画面
の生成と表示
S192
メニューへ
ボタン
ログアウト
B10
ログアウト通知
S193
ログアウト通知
S194
終了
S196
S195
ログイン情報の消去
ログイン情報の消去

図27

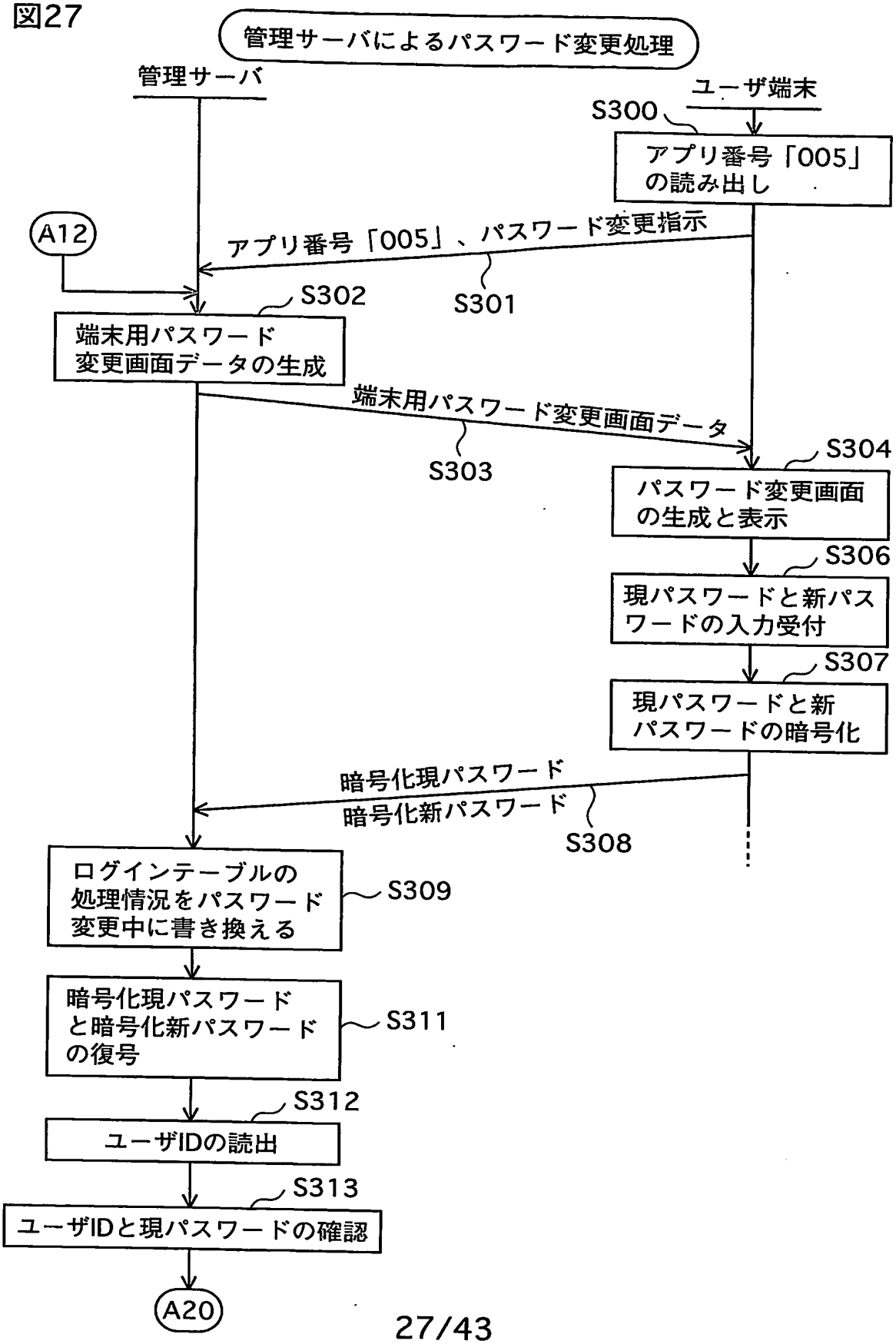

管理サーバによるパスワード変更処理
管理サーバ
ユーザ端末
S300
アプリ番号「005」の読み出し
A12
アプリ番号「005」、パスワード変更指示
S301
S302
端末用パスワード変更画面データの生成
端末用パスワード変更画面データ
S303
S304
パスワード変更画面の生成と表示
S306
現パスワードと新パスワードの入力受付
S307
現パスワードと新パスワードの暗号化
暗号化現パスワード
暗号化新パスワード
S308
ログインテーブルの処理情況をパスワード変更中に書き換える
S309
暗号化現パスワードと暗号化新パスワードの復号
S311
S312
ユーザIDの読出
S313
ユーザIDと現パスワードの確認
A20

図28

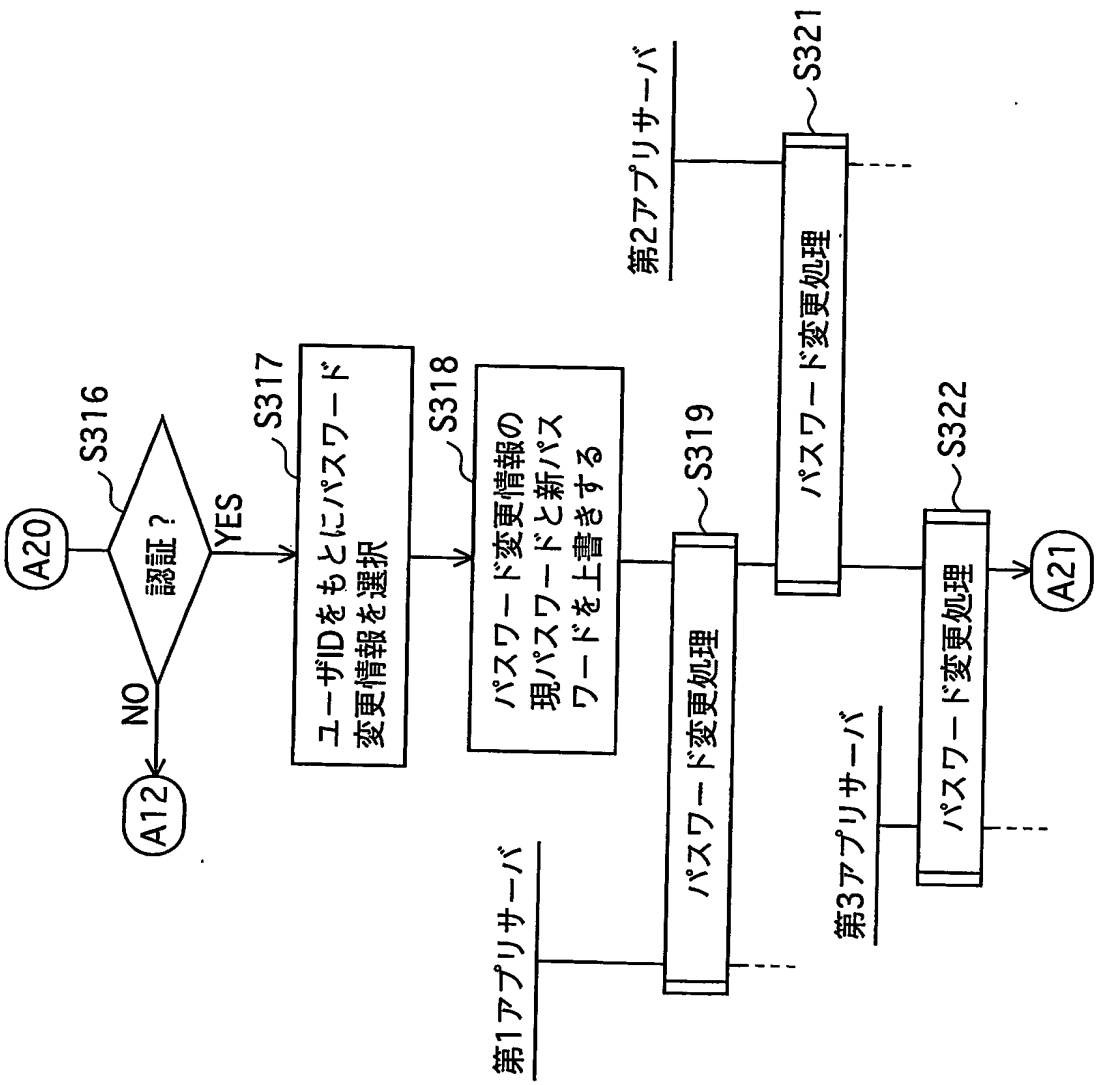

A20
S316
認証？
YES
NO
A12
S317
ユーザIDをもとにパスワード変更情報を選択
S318
パスワード変更情報の現パスワードと新パスワードを上書きする
S319
パスワード変更処理
第1アプリサーバ
第2アプリサーバ
S321
パスワード変更処理
第3アプリサーバ
S322
パスワード変更処理
A21

図29

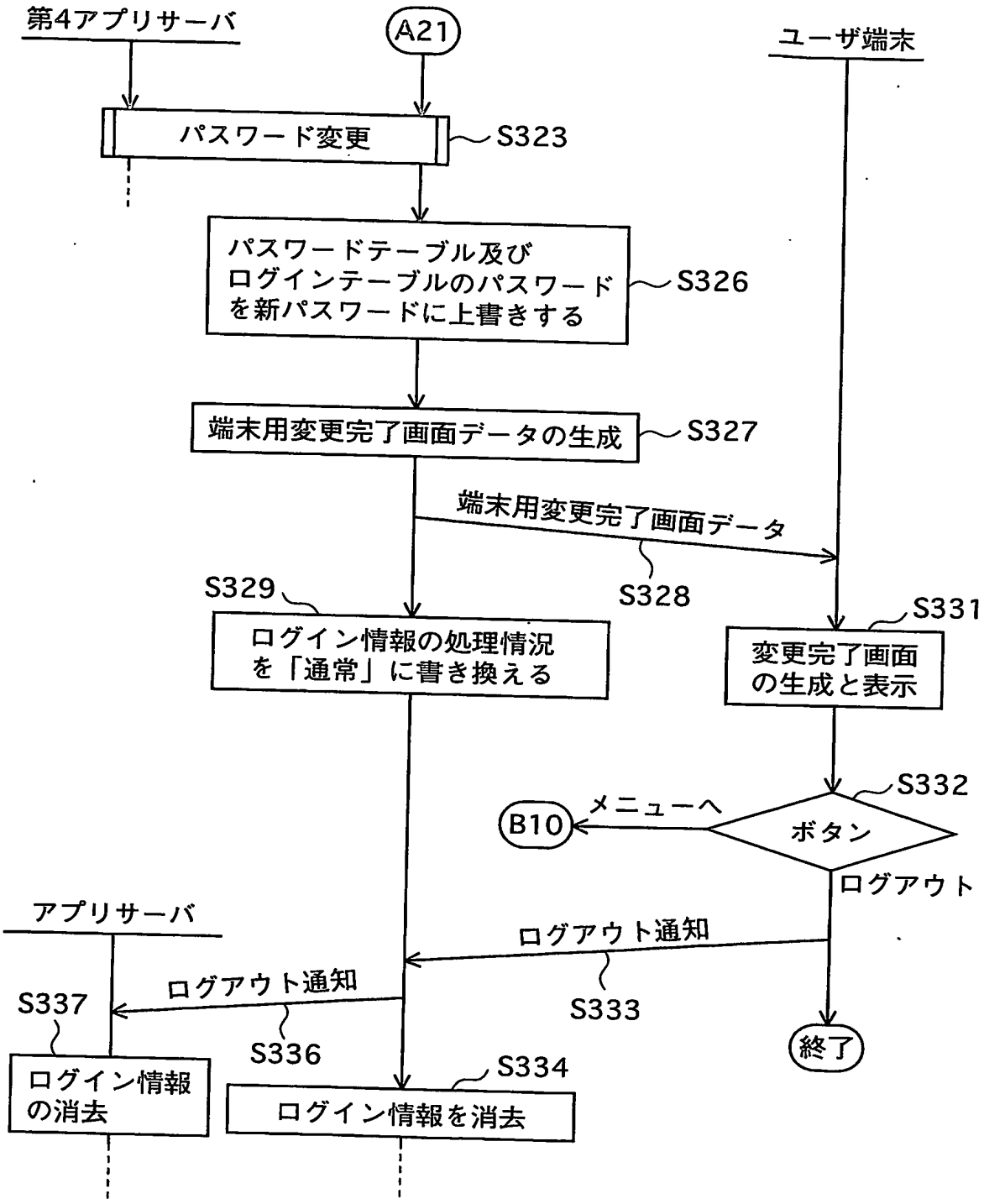

第4アプリサーバ
A21
ユーザ端末
パスワード変更
S323
パスワードテーブル及び
ログインテーブルのパスワード
を新パスワードに上書きする
S326
端末用変更完了画面データの生成
S327
端末用変更完了画面データ
S328
S329
ログイン情報の処理情況
を「通常」に書き換える
S331
変更完了画面
の生成と表示
S332
メニューへ
B10
ボタン
ログアウト
アプリサーバ
ログアウト通知
S333
ログアウト通知
S337
S336
終了
S334
ログイン情報
の消去
ログイン情報を消去

図30

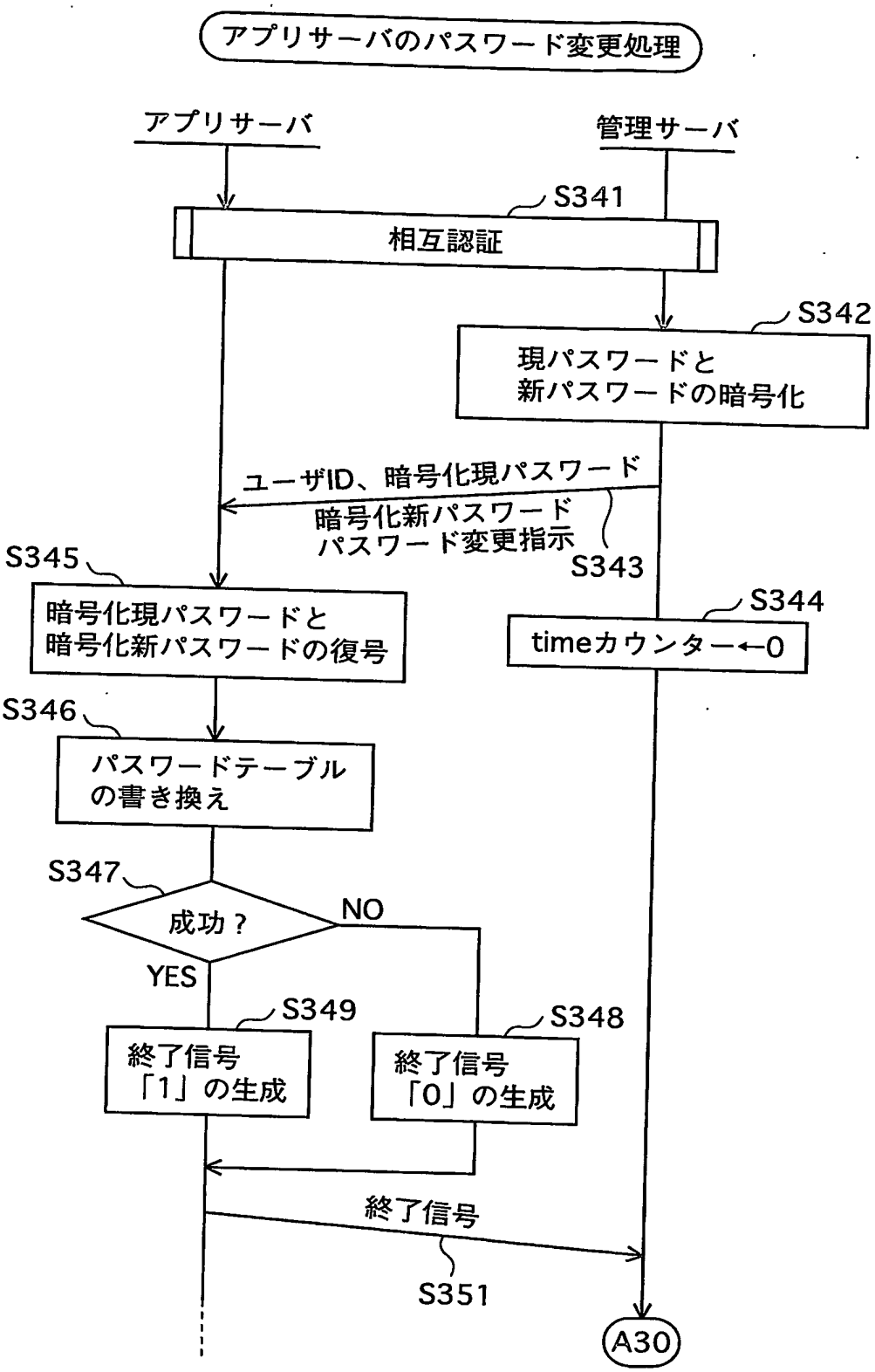

アプリサーバのパスワード変更処理
アプリサーバ
管理サーバ
S341
相互認証
S342
現パスワードと
新パスワードの暗号化
ユーザID、暗号化現パスワード
暗号化新パスワード
パスワード変更指示
S343
S345
暗号化現パスワードと
暗号化新パスワードの復号
S344
timeカウンター←0
S346
パスワードテーブル
の書き換え
S347
成功？
NO
YES
S349
終了信号
「1」の生成
S348
終了信号
「0」の生成
終了信号
S351
A30

図31

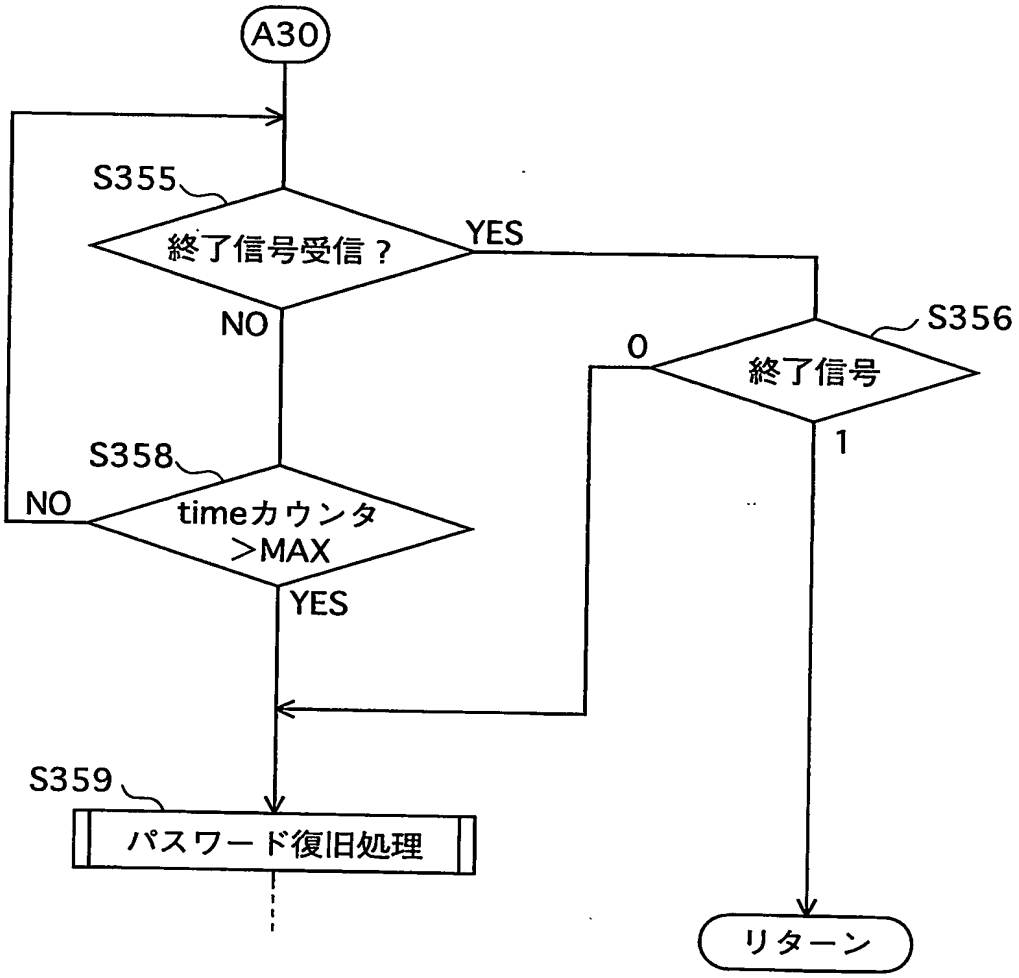

A30
S355
終了信号受信？
YES
NO
S356
0
終了信号
1
S358
NO
timeカウンタ
＞MAX
YES
S359
パスワード復旧処理
リターン

図32

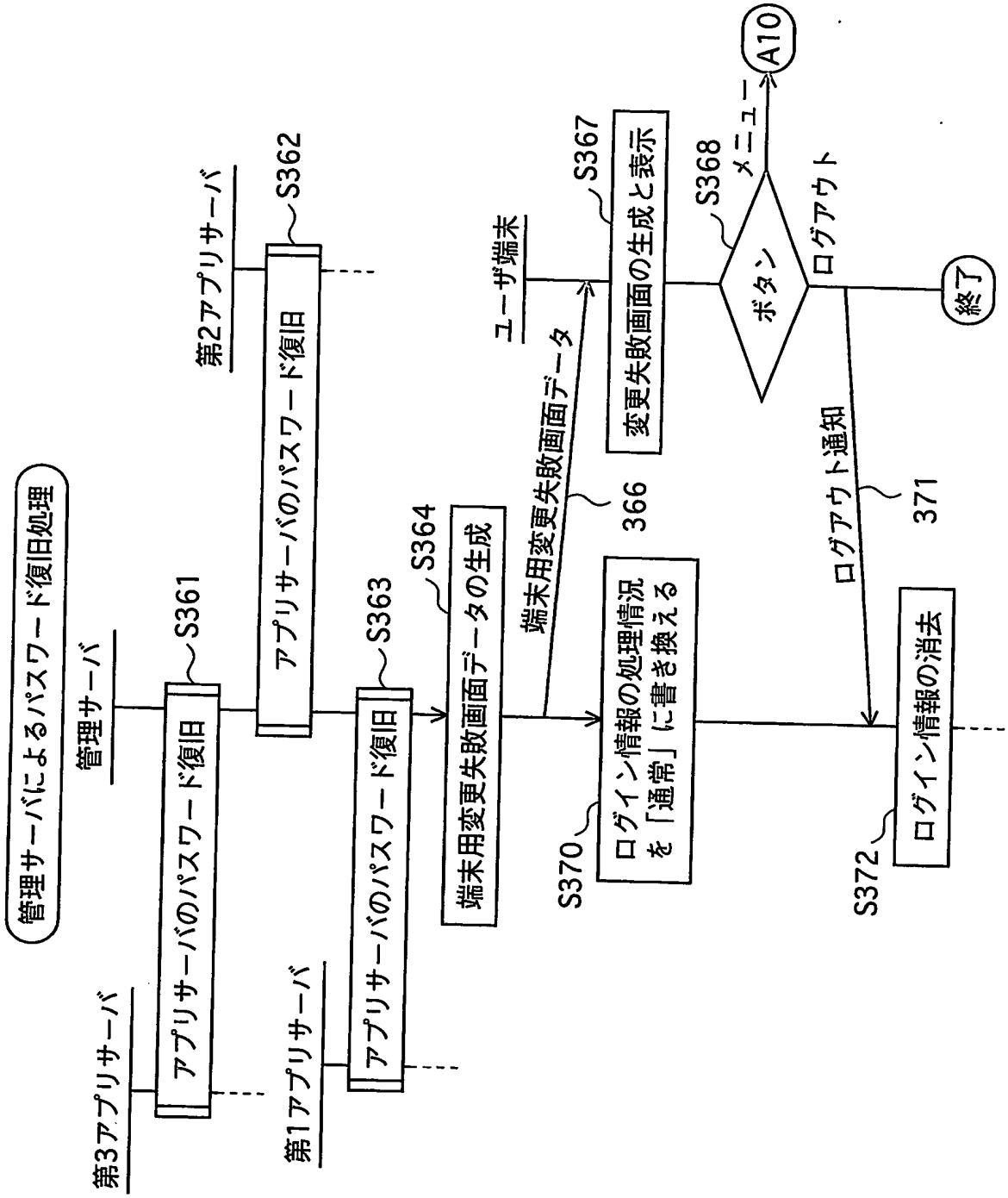

管理サーバによるパスワード復旧処理
管理サーバ
第3アプリサーバ
第2アプリサーバ
第1アプリサーバ
アプリサーバのパスワード復旧
S361
アプリサーバのパスワード復旧
S362
アプリサーバのパスワード復旧
S363
端末用変更失敗画面データの生成
S364
ユーザ端末
端末用変更失敗画面データ
366
変更失敗画面の生成と表示
S367
ボタン
S368
メニュー
A10
ログアウト
終了
ログアウト通知
371
ログイン情報の処理情況を「通常」に書き換える
S370
ログイン情報の消去
S372

図33

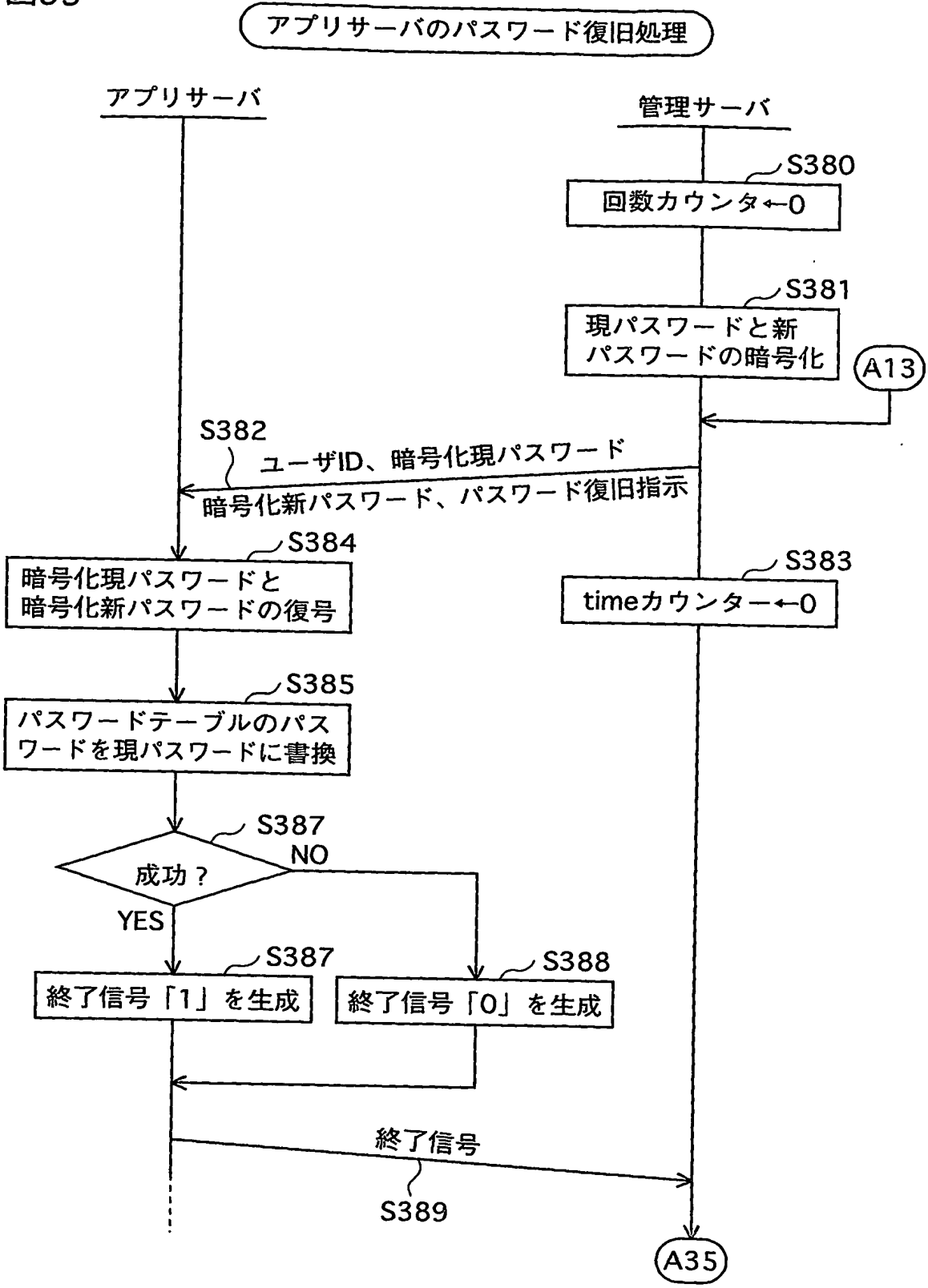

アプリサーバのパスワード復旧処理
アプリサーバ
管理サーバ
S380
回数カウンタ←0
S381
現パスワードと新パスワードの暗号化
A13
S382
ユーザID、暗号化現パスワード
暗号化新パスワード、パスワード復旧指示
S384
暗号化現パスワードと暗号化新パスワードの復号
S383
timeカウンター←0
S385
パスワードテーブルのパスワードを現パスワードに書換
S387
成功？
NO
YES
S387
終了信号「1」を生成
S388
終了信号「0」を生成
終了信号
S389
A35

図34

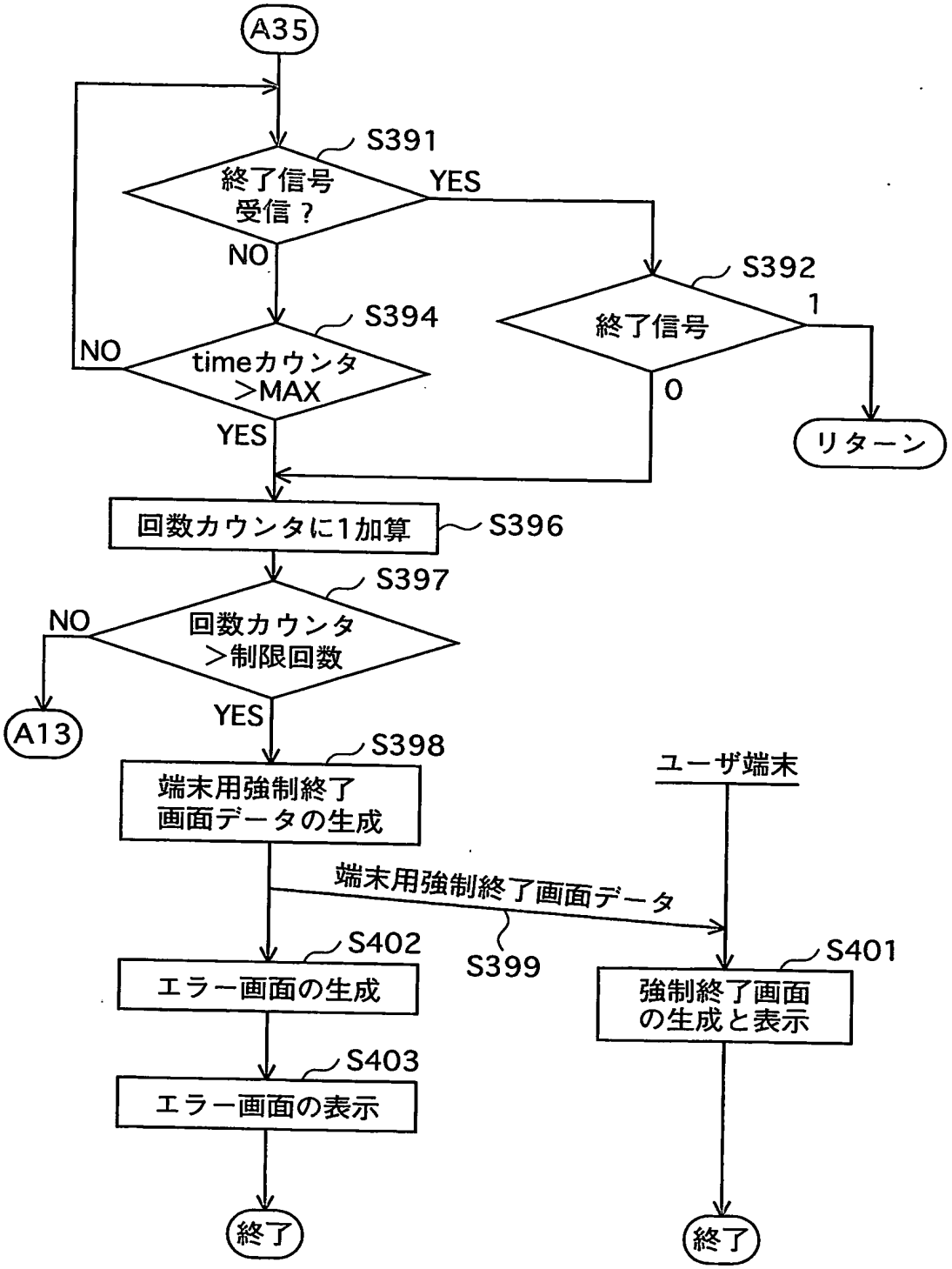

A35
S391
終了信号
受信？
YES
NO
S392
終了信号
1
0
S394
timeカウンタ
＞MAX
NO
YES
リターン
回数カウンタに1加算
S396
S397
回数カウンタ
＞制限回数
NO
YES
A13
S398
端末用強制終了
画面データの生成
ユーザ端末
端末用強制終了画面データ
S399
S402
エラー画面の生成
S401
強制終了画面
の生成と表示
S403
エラー画面の表示
終了
終了

図35

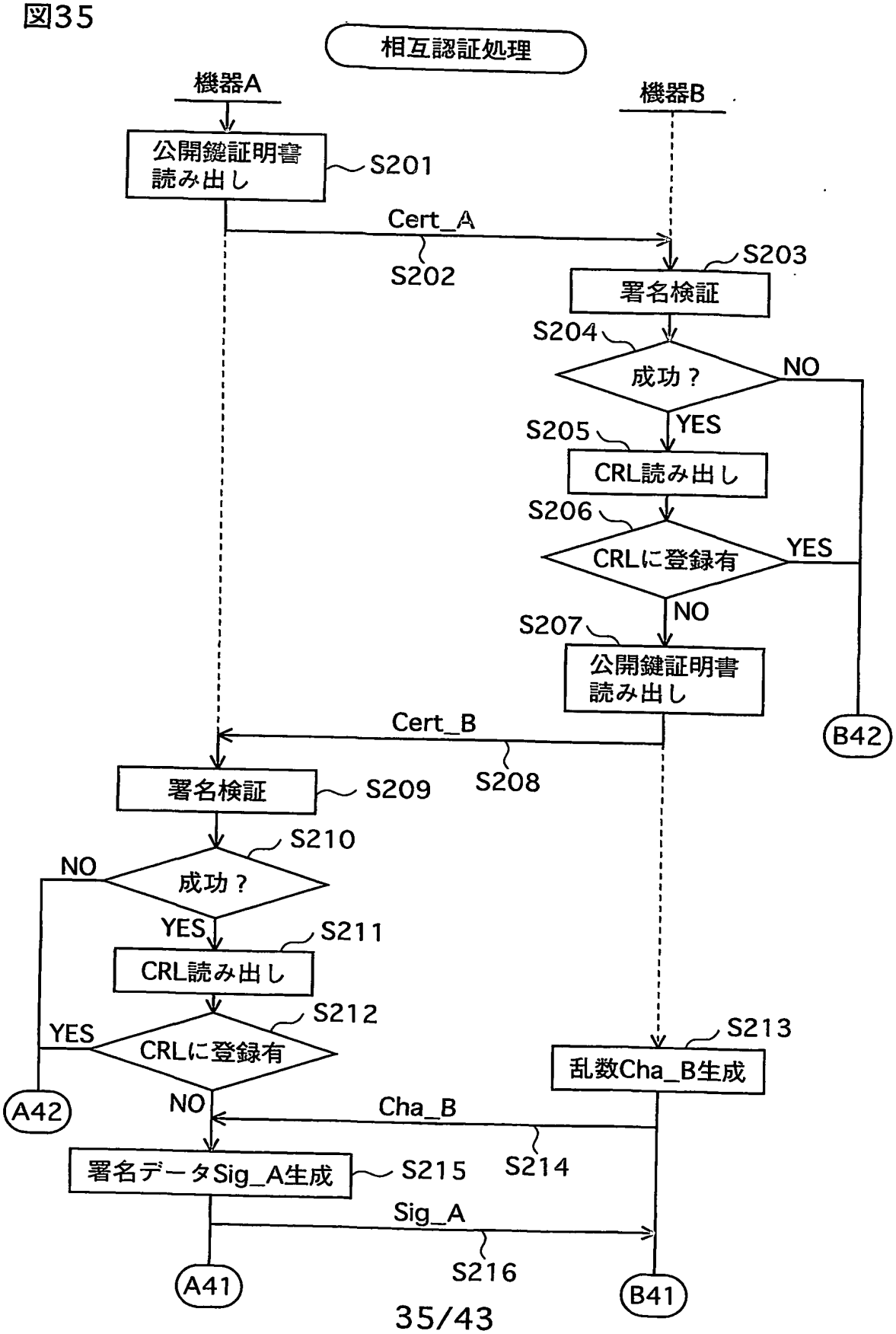

相互認証処理
機器A
機器B
公開鍵証明書読み出し
S201
Cert_A
S202
S203
署名検証
S204
成功？
NO
YES
S205
CRL読み出し
S206
CRLに登録有
YES
NO
S207
公開鍵証明書読み出し
B42
Cert_B
S208
署名検証
S209
S210
NO
成功？
YES
S211
CRL読み出し
S212
YES
CRLに登録有
A42
S213
乱数Cha_B生成
NO
Cha_B
S214
署名データSig_A生成
S215
Sig_A
S216
A41
B41

図36

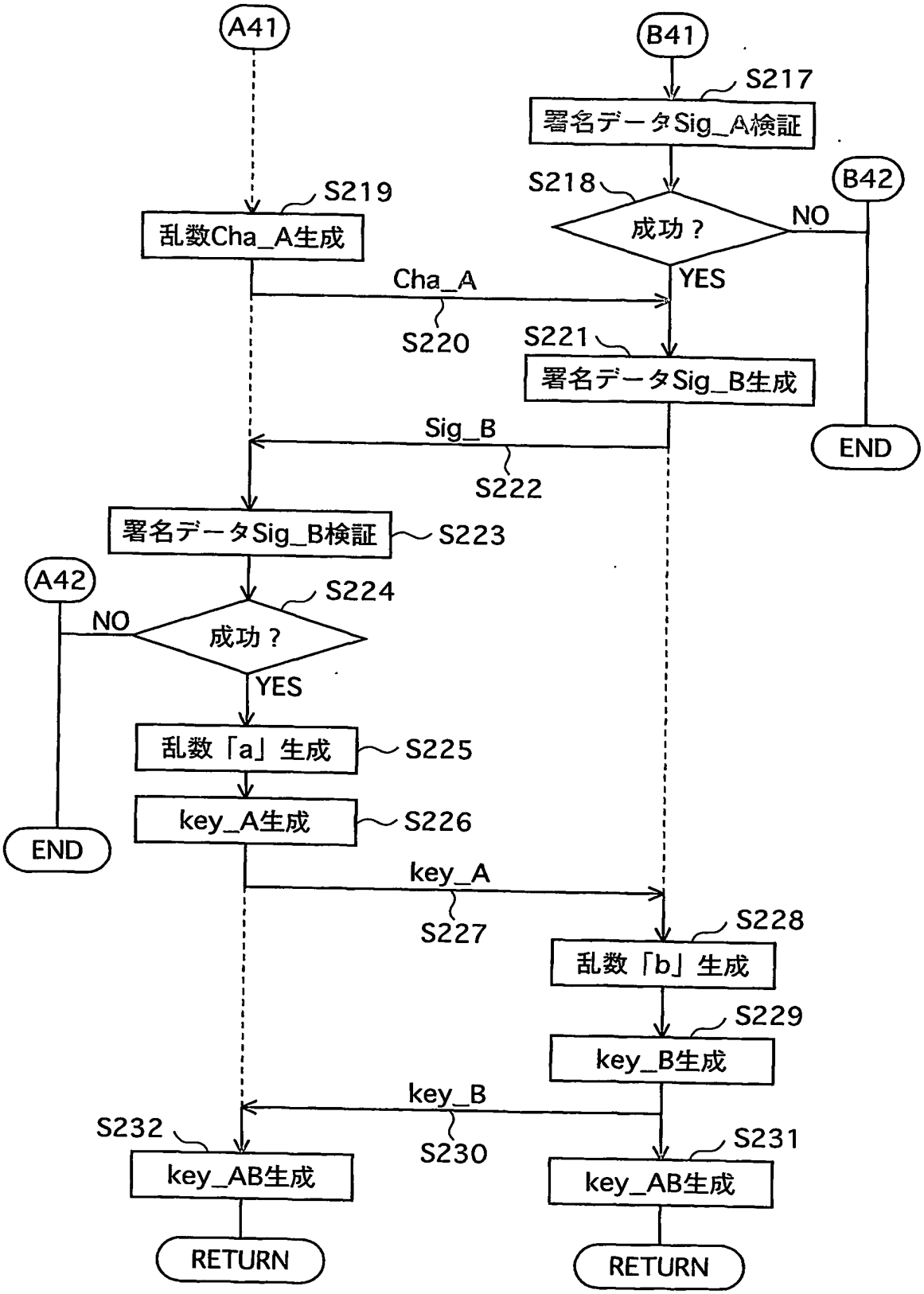

A41
B41
S217
署名データSig_A検証
S218
成功？
NO
B42
YES
S219
乱数Cha_A生成
Cha_A
S220
S221
署名データSig_B生成
END
Sig_B
S222
署名データSig_B検証
S223
A42
S224
NO
成功？
YES
乱数「a」生成
S225
key_A生成
S226
END
key_A
S227
S228
乱数「b」生成
S229
key_B生成
key_B
S230
S232
S231
key_AB生成
key_AB生成
RETURN
RETURN

図37

(a)

アプリサーバ名	第1アプリサーバ	第2アプリサーバ	第3アプリサーバ	第4アプリサーバ
パスワード	ozy12	ozy12	ozy12	ozy12

(b)

アプリサーバ名	第1アプリサーバ	第2アプリサーバ	第3アプリサーバ	第4アプリサーバ
パスワード	nwy56	nwy56	ozy12	ozy12

(c)

アプリサーバ名	第1アプリサーバ	第2アプリサーバ	第3アプリサーバ	第4アプリサーバ
パスワード	ozy12	ozy12	ozy12	ozy12

(d)

アプリサーバ名	第1アプリサーバ	第2アプリサーバ	第3アプリサーバ	第4アプリサーバ
パスワード	nwy56	nwy56	nwy56	nwy56

図38

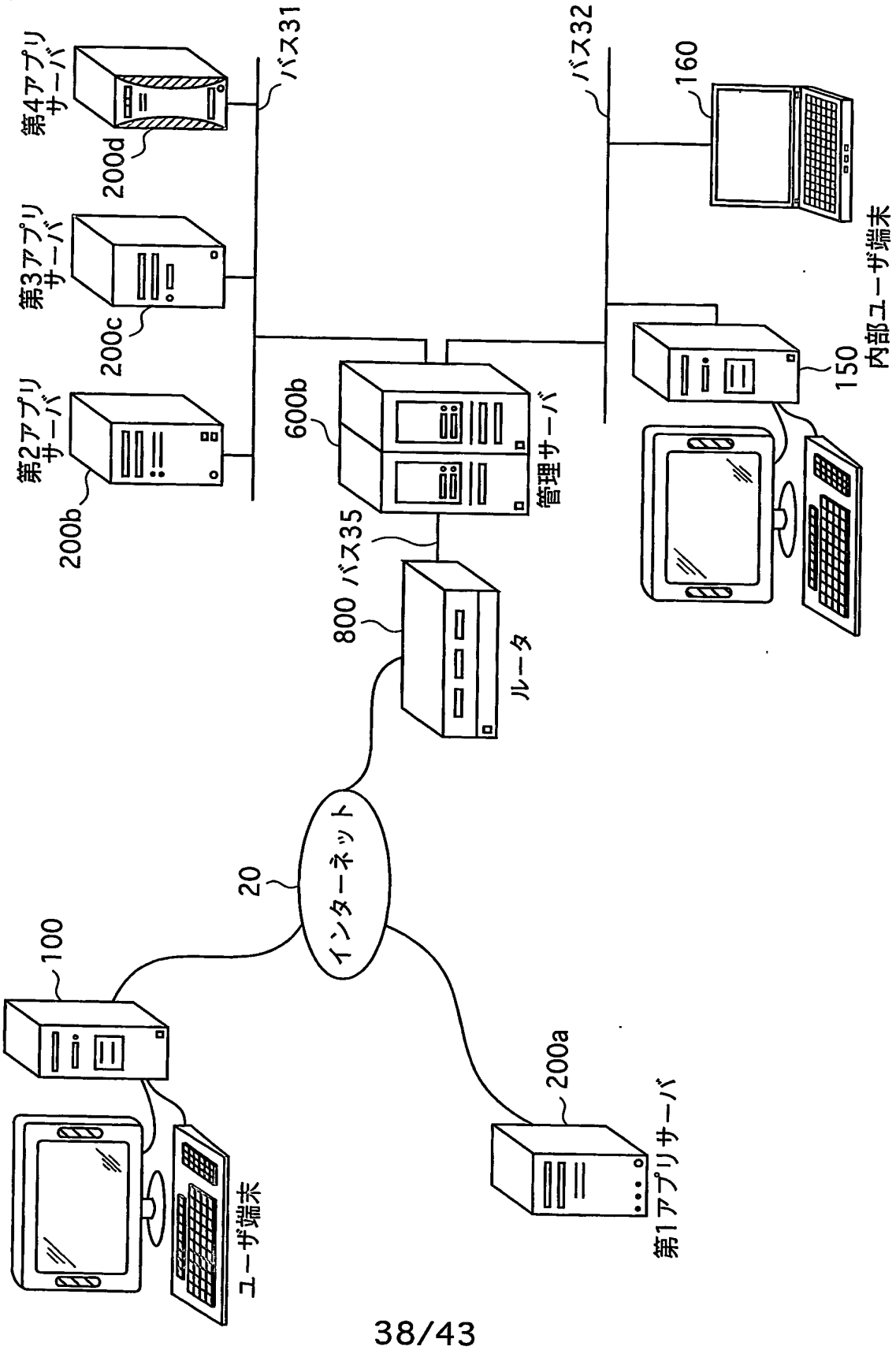

第4アプリサーバ
200d
第3アプリサーバ
200c
第2アプリサーバ
200b
バス31
バス32
160
内部ユーザ端末
150
600b
管理サーバ
800
バス35
ルータ
20
インターネット
100
ユーザ端末
200a
第1アプリサーバ

図39

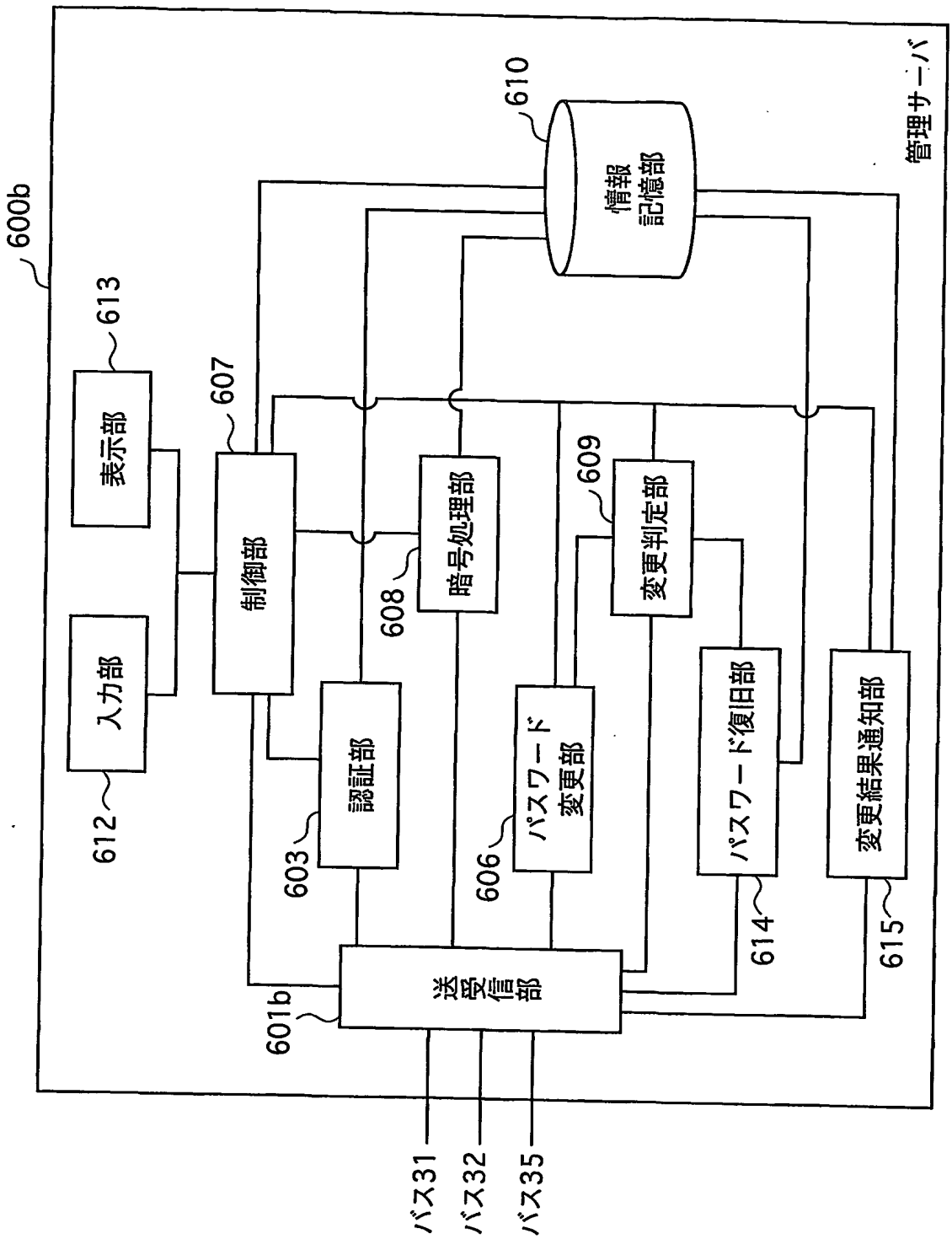

600b
管理サーバ
610
情報記憶部
613
表示部
607
制御部
608
暗号処理部
609
変更判定部
入力部
612
認証部
603
パスワード変更部
606
パスワード復旧部
614
変更結果通知部
615
601b
送受信部
バス31
バス32
バス35

図40

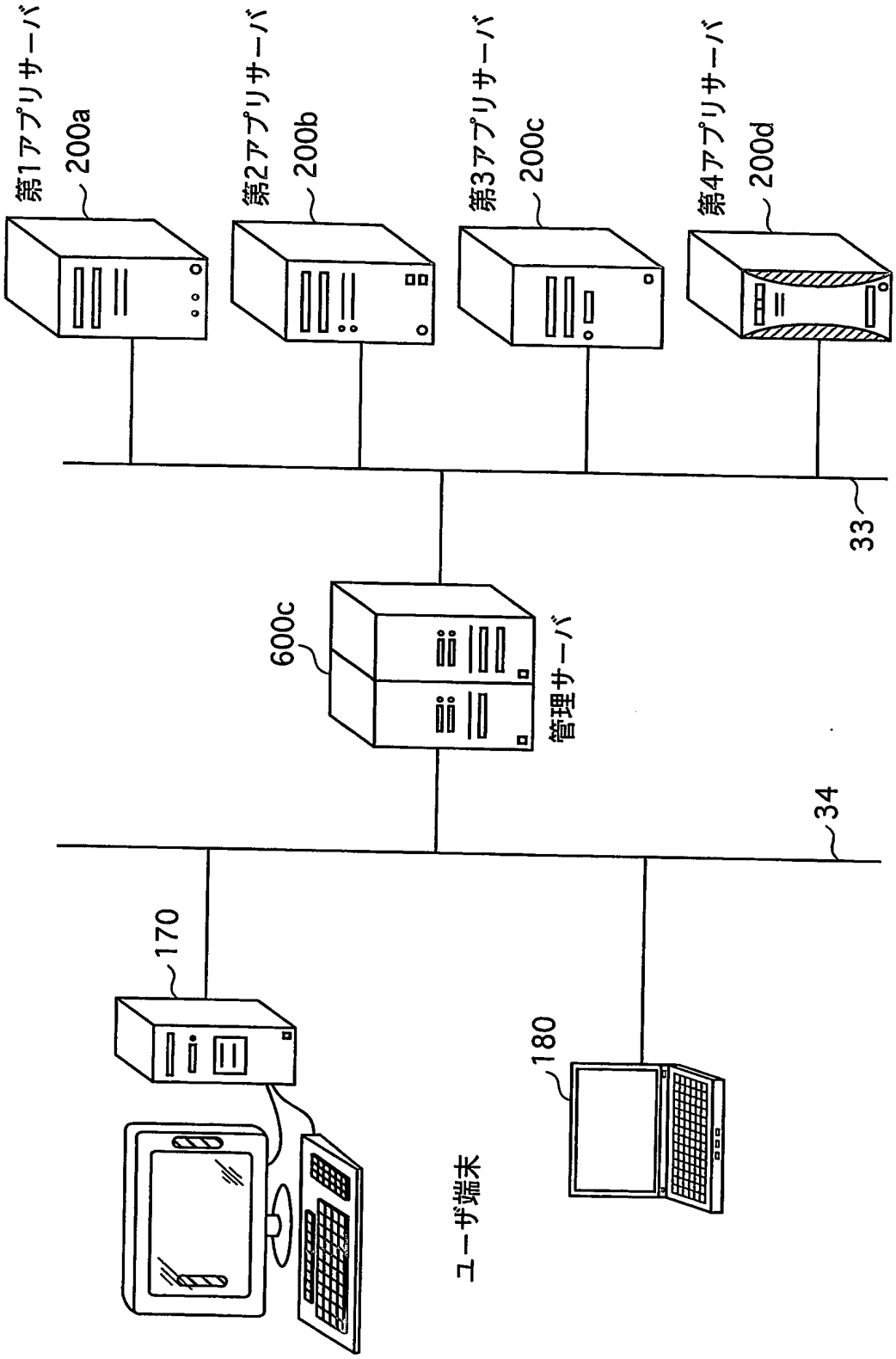

第1アプリサーバ
200a
第2アプリサーバ
200b
第3アプリサーバ
200c
第4アプリサーバ
200d
33
600c
管理サーバ
34
170
180
ユーザ端末

図41

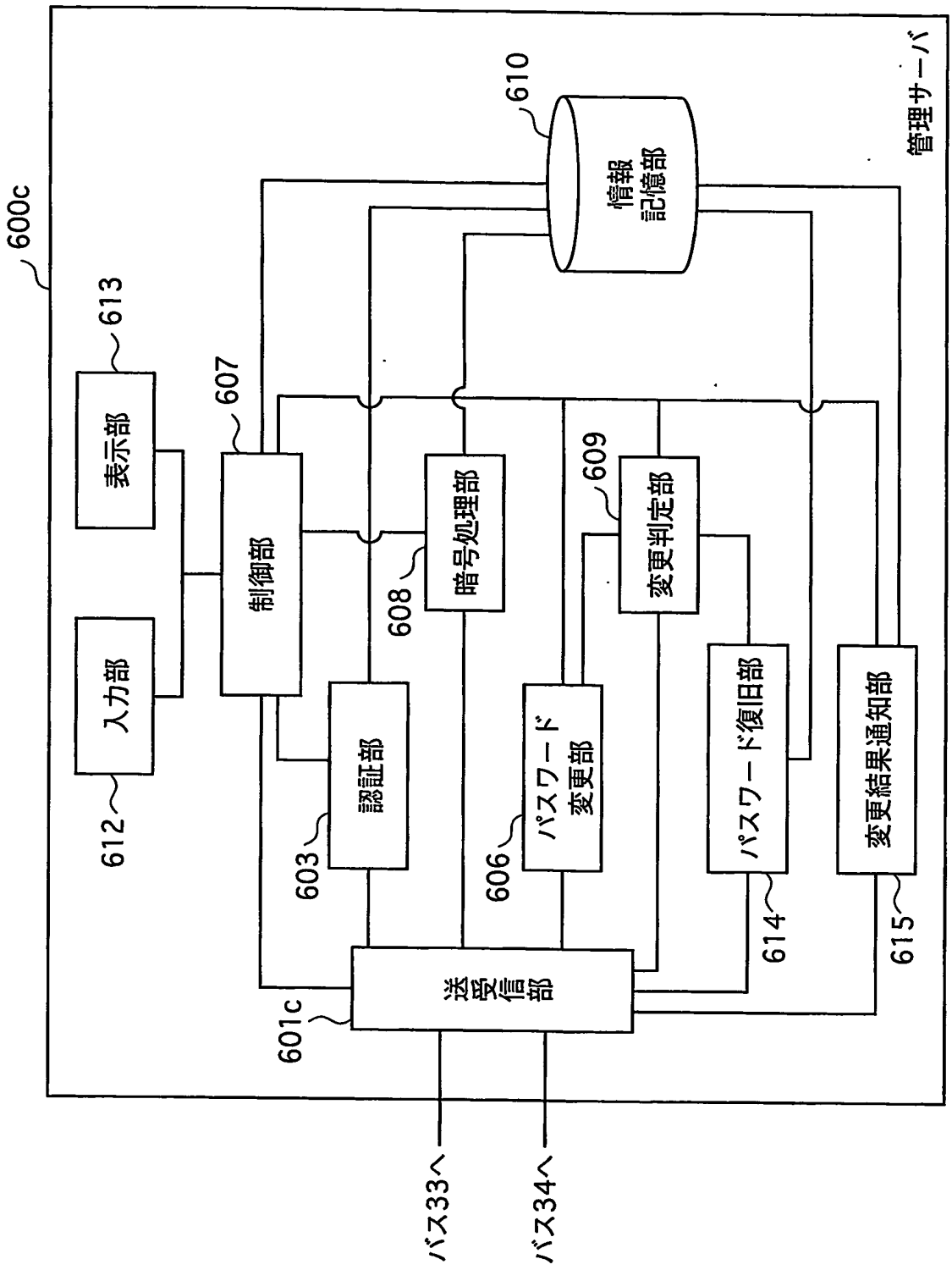

600c
管理サーバ
610
情報記憶部
613
表示部
607
制御部
608
暗号処理部
609
変更判定部
612
入力部
603
認証部
606
パスワード変更部
614
パスワード復旧部
615
変更結果通知部
601c
送受信部
バス33へ
バス34へ

図42

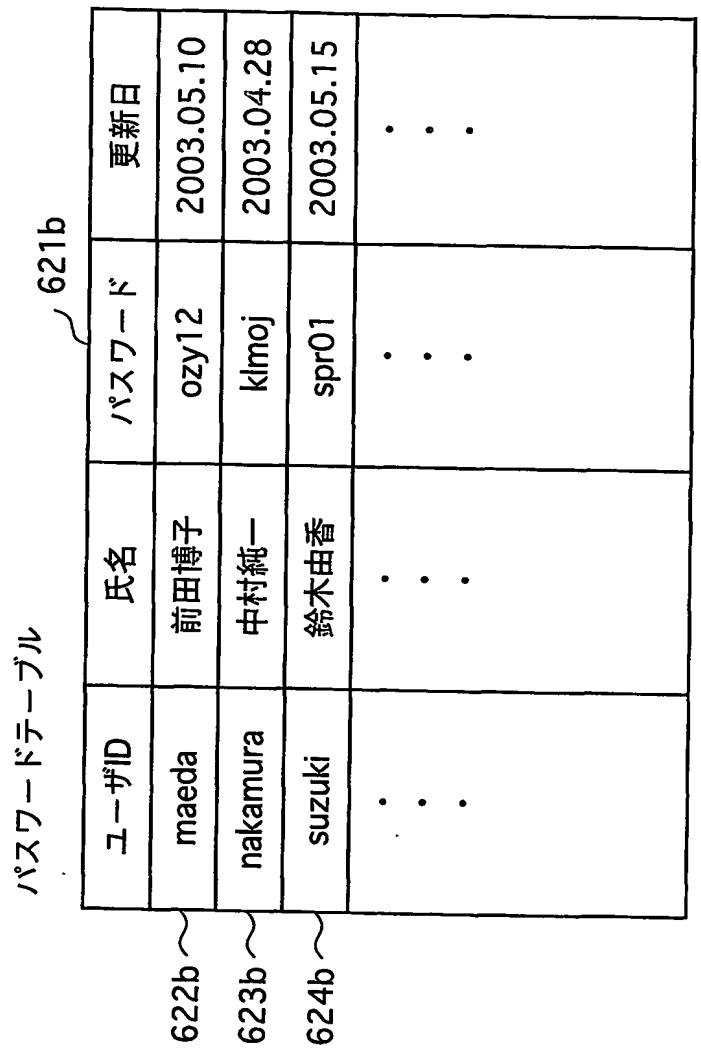
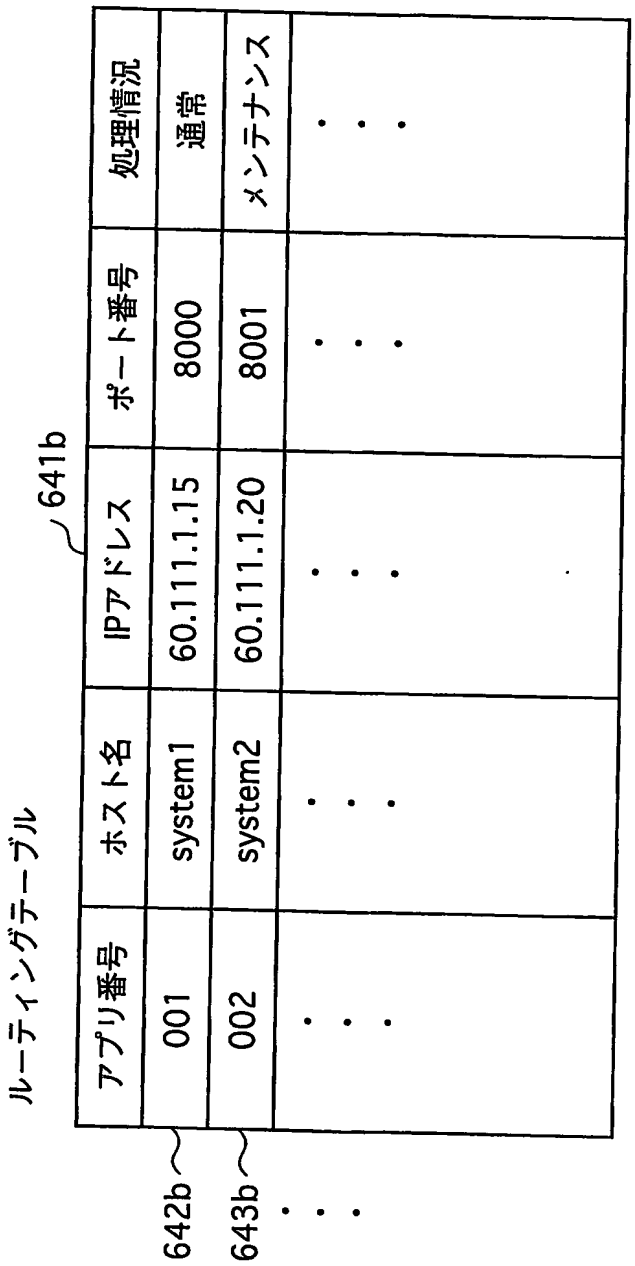

パスワードテーブル
621b
ユーザID
氏名
パスワード
更新日
maeda
前田博子
ozy12
2003.05.10
nakamura
中村純一
klmoj
2003.04.28
suzuki
鈴木由香
spr01
2003.05.15
622b
623b
624b

図43


ルーティングテーブル
641b
アプリ番号
ホスト名
IPアドレス
ポート番号
処理情況
001
system1
60.111.1.15
8000
通常
002
system2
60.111.1.20
8001
メンテナンス
642b
643b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/005205

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, H04L9/32, G06F13/00, G06F1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS): Japanese
Computer Software Data Base (Japanese Patent Office): Japanese

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-043189 A (PFU Ltd.), 16 February, 2001 (16.02.01), Figs. 4 to 7 and their explanations (Family: none)	1-35
Y	Atsushi IIZAWA et al., "Database Omoshiro Koza", 1st edition, Kyoritsu Shuppan Co., Ltd., 30 April, 1993 (30.04.93), ISBN:4-320-02640-3, pages 189 to 210 (in particular, Fig. 10-4 in page 203)	1-35

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 10 May, 2004 (10.05.04)	Date of mailing of the international search report 25 May, 2004 (25.05.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/005205

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Philip A. Berstein et al., translated by Kazuhiro OISO et al., "Transaction Shori System Nyumon", 1st edition, Nikkei Business Publications, Inc., 23 March, 1998 (23.03.98), ISBN:4-8222-8026-8, pages 13 to 16 and 256 to 279 (in particular, page 259, messages of "preparation request", "preparation completion" in Fig.9.1; page 262, messages of "preparation completion", "rejection" and descriptions concerning "time-out" on lines 12 to 16)	7-10
Y	JP 9-016502 A (Fujitsu Ltd.), 17 January, 1997 (17.01.97), Page 3, left column, pages 34 to 37 (Family: none)	12,13,22
Y	A.S. Tanenbaum, translated by Nobuyuki HIKICHI et al., "OS no Kiso to Oyo", 1st edition, Kabushiki Kaisha Toppan, 30 November, 1995 (30.11.95), ISBN:4-8101-8543-5, pages 460 to 462 (descriptions concerning name-server)	17
Y	Hirokazu NOBUKUNI et al., "Web to Mail de Seikyu Joho o Shokai Dekiru Web Billing", NTT Gijutsu Journal, 01 November, 2001 (01.11.01), ISSN:0915-2318, pages 94 to 97 (in particular, page 96, center column, line 15 to right column, line 1)	19

国際調査報告

国際出願番号　PCT／JP2004／005205

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F15／00, H04L9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F15／00, H04L9／32, G06F13／00, G06F1／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2004年
日本国登録実用新案公報　1994－2004年
日本国実用新案登録公報　1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTファイル（JOIS）：日本語
Computer Software Data Base（日本国特許庁）：日本語

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　2001－043189　A（株式会社ピーエフユー）2001．02．16，図4－図7とその説明文（ファミリーなし）	1－35
Y	飯沢篤志、外1名，データベースおもしろ講座，初版，共立出版株式会社，1993．04．30，ISBN:4-320-02640-3，pp．189－210（特に第203頁の図10－4）	1－35

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
10．05．2004	25．5．2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	久保　光宏	5B	9189
	電話番号　03－3581－1101　内線　3546		

様式PCT／ISA／210（第2ページ）（2004年1月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００５２０５

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	フィリップ・Ａ・バーンスタイン、外１名著， 大磯和広、外４名訳，トランザクション処理システム入門，初版， 日経ＢＰ社，１９９８．０３．２３，ISBN:4-8222-8026-8， ｐｐ．１３－１６及び２５６－２７９（特に第２５９頁の 図９．１の「準備要求」、「準備完了」メッセージと、 第２６２頁第１２－１６行の「準備完了」、「拒否」メッセージと 「時間切れ」に関する記述）	７－１０
Ｙ	ＪＰ　９－０１６５０２　Ａ（富士通株式会社） １９９７．０１．１７，第３頁左欄第３４－３７行 （ファミリーなし）	１２，１３， ２２
Ｙ	Ａ．Ｓ．タネンバウム著，引地信之、外１名訳， ＯＳの基礎と応用，初版，株式会社トッパン， １９９５．１１．３０，ISBN:4-8101-8543-5， ｐｐ．４６０－４６２（ネーム・サーバに関する記載）	１７
Ｙ	信國浩一、外３名，Ｗｅｂとメールで請求情報を照会できるＷｅｂ Ｂｉｌｌｉｎｇ，ＮＴＴ技術ジャーナル，２００１．１１．０１， ISSN:0915-2318，ｐｐ．９４－９７（特に第９６頁中央欄第１５行 －同頁右欄第１行）	１９